Secure e-voting System using Blockchain

A major project report submitted in partial fulfillment of the requirement for the award of degree of

Bachelor of Technology

in

Computer Science & Engineering

Submitted by

Lakshika Gupta (201261)

Priyanjana Srivastava (201212)

Under the guidance & supervision of

Prof. Dr. Pradeep Kumar Gupta

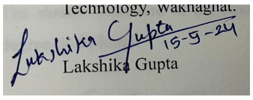
Department of Computer Science & Engineering and Information Technology

Jaypee University of Information Technology,

Waknaghat, Solan - 173234 (India)

CERTIFICATE

This is to certify that the work which is being presented in the project report titled “Secure e-voting System using Blockchain” in partial fulfillment of the requirements for the award of the degree of B.Tech in Computer Science And Engineering and submitted to the Department of Computer Science And Engineering, Jaypee University of Information Technology, Waknaghat is an authentic record of work carried out by “Lakshika Gupta, 201261” and “Priyanjana Srivastava, 201212” during the period from August 2023 to May 2024 under the supervision of Prof. Dr. Pradeep Kumar Gupta, Department of Computer Science and Engineering, Jaypee University of Information Technology, Waknaghat.



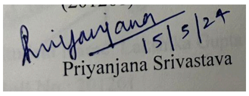
Technology, Waknaghat.

Lakshika Gupta 15-5-24

Lakshika Gupta

Lakshika Gupta

(201261)



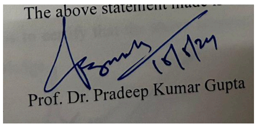
Priyanjana 15/5/24

Priyanjana Srivastava

Priyanjana Srivastava

(201212)

The above statement made is correct to the best of my knowledge.



The above statement

15/5/24

Prof. Dr. Pradeep Kumar Gupta

Prof. Dr. Pradeep Kumar Gupta

Professor

Computer Science & Engineering and Information Technology

Jaypee University of Information Technology, Waknaghat

CANDIDATE'S DECLARATION

We hereby declare that the work presented in this report entitled **'Secure e-voting System using Blockchain'** in partial fulfillment of the requirements for the award of the degree of **Bachelor of Technology** in **Computer Science & Engineering** submitted in the Department of Computer Science & Engineering and Information Technology**,** Jaypee University of Information Technology, Waknaghat is an authentic record of my own work carried out over a period from August 2023 to May 2024 under the supervision of **Prof. Dr. Pradeep Kumar Gupta**(Professor, Department of Computer Science & Engineering and Information Technology).

The matter embodied in the report has not been submitted for the award of any other degree or diploma.

Technology, Waknaghat.
Lakshika Gupta 15-5-24
Lakshika Gupta

Priyanjana 15/5/24
Priyanjana Srivastava

Student Name: Lakshika Gupta
Roll No.: 201261

Student Name: Priyanjana Srivastava
Roll No.: 201212

This is to certify that the above statement made by the candidate is true to the best of my knowledge.

The above statement made
15/5/24
Prof. Dr. Pradeep Kumar Gupta

Supervisor Name: Prof. Dr. Pradeep Kumar Gupta
Designation: Professor
Department: Computer Science & Engineering and Information Technology
Dated: May 15, 2024

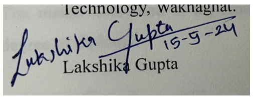
ACKNOWLEDGMENT

Firstly, I express my heartiest thanks and gratefulness to almighty God for His divine blessing makes us possible to complete the project work successfully. I really grateful and wish my profound my indebtedness to Supervisor Prof. Dr. Pradeep Kumar Gupta, Professor, Department of CSE Jaypee University of Information Technology, Waknaghat. Deep Knowledge & keen interest of my supervisor in the field of "Research Area" to carry out this project. Her endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior drafts and correcting them at all stage have made it possible to complete this project.

I would like to express my heartiest gratitude to Prof. Dr. Pradeep Kumar Gupta, Department of CSE, for his kind help to finish my project.

I would also generously welcome each one of those individuals who have helped me straight forwardly or in a roundabout way in making this project a win. In this unique situation, I might want to thank the various staff individuals, both educating and non-instructing, which have developed their convenient help and facilitated my undertaking.

Finally, I must acknowledge with due respect the constant support and patients of my parents.



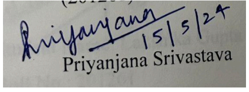
Technology, Waknaghat.

Lakshika Gupta 15-5-24

Lakshika Gupta

Lakshika Gupta

(201261)



Priyanjana 15/5/24

Priyanjana Srivastava

Priyanjana Srivastava

(201212)

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS, SYMBOLS, OR NOMENCLATURE

ABBREVIATIONS	DEFINITIONS
IJRASET	International Journal for Research in Applied Science and Engineering Technology.
IEEE	Institute of Electrical and Electronics Engineers.
GCAT	Global Conference for Advancement in Technology.
ICECCO	International Conference on Electronics Computer and Computation.
EVM	Electronic Voting Machine.
DDoS	Distributed Denial of Service.
SHA-256	Secure Hash Algorithm.
OCR	Optical Character Recognition.

ABSTRACT

The principle underlying elections is that representatives should be elected at elections on behalf of electoral law, justice, and integrity. The voting method allows approved voters to vote for candidates in an election. In essence, the voting system influences numerous issues in politics and society, science, and economics fields. These should be thought and addressed carefully. It is the most widespread method in international setting. A second instrument of electoral democracy is e-voting. Nonetheless, the most countries still need to work hard on that aspect. Even yet, the present voting system does not meet many expectation.Blockchain technology eliminates decentralized architecture that distributes information simultaneously. For this, we can thank technology that tackles problem these includes “perfect online privacy” and Platform 3.0 dApps among other concepts associated with blockchain. Consequently, the analysis reveals that can be developed using a blockchain enhances the transparency of the voting system, and also increases its legitimacy and efficiency,consistent voting, for example, in the voting process and producing the same number of votes. Lastly, the study discussed to identify some challenges in today’s voting methodology and apply block chain technology, addresses such drawbacks.

CHAPTER 1:INTRODUCTION

1.1 INTRODUCTION:

First and foremost, there are paper voting and e-voting schemes, all of which require voters to go to a designated polling place to cast their ballots. After the polling procedure, the paper vote counting system was used, which was performed manually or by machine (physical counting). E-voting, on the other hand, keeps track of each vote as it is counted. The next step will be to combine all of the candidate counts from the polling stations, which would be the same for all of the elections. Since 1999, India has been one of the countries that has used electronic voting machines (EVMs) in elections. When opposed to other e-voting companies in India, EVMs are unquestionably more cost-effective. I-voting allows electors to vote from anywhere via a browser (web application) or a mobile application.

What does blockchain do?

An alternative to centralized services is a blockchain which is a peer-to-peer system without a central authority in charge of managing data flows. One of the other principal roles the distributed, comprehensive network of different users could have is to help keep data integrity without any central control. It is that the computers that form the network are in more than one place. These machines are formally known as full nodes in crypto space.

A cryptocurrency is a virtual asset that is traded on the market and has a cash value. Cryptocurrencies are traded on exchanges just like stocks. Cryptocurrencies run on a separate blockchain for each company. The software is what gives the hardware use. The software is the blockchain protocol. The widely known protocols among blockchain protocols are Bitcoin, Ethereum, and Ripple. The implementation consist of a main hardware architecture with full nodes which are securing the data in a network.

The heart of the democratic institutions lies on the truth and the open presentation of the elections. This can be accomplished by offering voters free and easy access into polls which are problem-free and barrier-free including providing for physical access and many other ways. Finally but importantly, a thorough evaluation will be on the cost element of the election process. It should be enough for everyone who is eligible to run for the elections, without the candidates being rated by wealth. Lastly, but not the least, voters should have a medium that enables them to cross-check that their votes have been registered correctly and tabulated properly which will eventually help in increasing trust in that process. The security of the integrity of elections is accomplished if people`s votes could not be changed, which also prevents abuse of the process and each voter`s decision be ignored.

Citizen-backed vote-breaking method has been confronted with opposition for years, particularly because of the security breaches and audit issues. Afterwards, voting via the internet was presented as an answer to problems, which may at least deal with some of them. From a good side, it is seen blockchain has a number of very pivotal changes, however a lot of worries are also rising concerning, for example, the possibility of DDoS attacks that can be seen to blockchain as a threat and also reason for its caution while talking about the reliability of the technology.

Lastly, the blockchain technology is the finalist of the e-voting issues, but that specific one can outshine the other. Blockchain as the secure, transparent, and decentralized technology is the primarily feature that makes it the suitable apparatus in making a trustworthy and audited voting system. In contrast to the scenario that election results were falsified before some elections were stolen due to the process that was not transparent, using cryptography in this new system to link the transactions and a distributed consensus mechanism this incorruptible chain of custody for votes is provided by eliminating the possibility of tampering or manipulation.

The very nature of blockchain networks as well as their governance algorithms is disperse, which in turn makes them more secure when they are used in centralized systems. Permanent research initiatives continue to try and investigate the blockchain technology in further detail so that they can understand how it can revolutionize automated voting systems. The goals of this enhancement are to show the strengthening of integrity, transparency, and accountability through the provision of predictable, reliable, and credible elections, all of which for a guaranteeing and thriving democracy.

What is Blockchain?

In the beginning, blockchain was just a computer science term for how to organize and share data. Blockchains are a new paradigm in Distributed Ledger Technology. Innovation is the process of combining old technology with new styles. Blockchains are a type of distributed databases that are controlled by a group of people and that store and share information. There are many differences in the types of blockchain and the blockchain applications. Blockchain is an innovative technology, which is implemented in different platforms and in all parts of the world as well.

A blockchain is a data structure that allows the creation of a digital ledger of data and its sharing among a network of independent parties. There are several different forms of blockchains. Every kind of a blockchain prevents a central authority from enforcing rules employing cryptography to make the ledger available and secure to each of the participants of a given network. The taking out of central authority from database structures is one of the most important and powerful features of blockchains.

Blockchains make records permanent and also store all the histories of transactions but nothing last forever. The shelf life of the record is grounded on the endurance of the network. In the case of blockchains, this means that a large part of a blockchain community would have to agree to change the information and are therefore not incentivized to change the data.

When data is recorded in a blockchain, it cannot be changed or removed in a very easy way. Validation control users either individually or collaboratively verify transactions proposed to be added to the blockchain. This is the point where things become complicated because each blockchain has its own approach to this issue and who can validate a transaction.

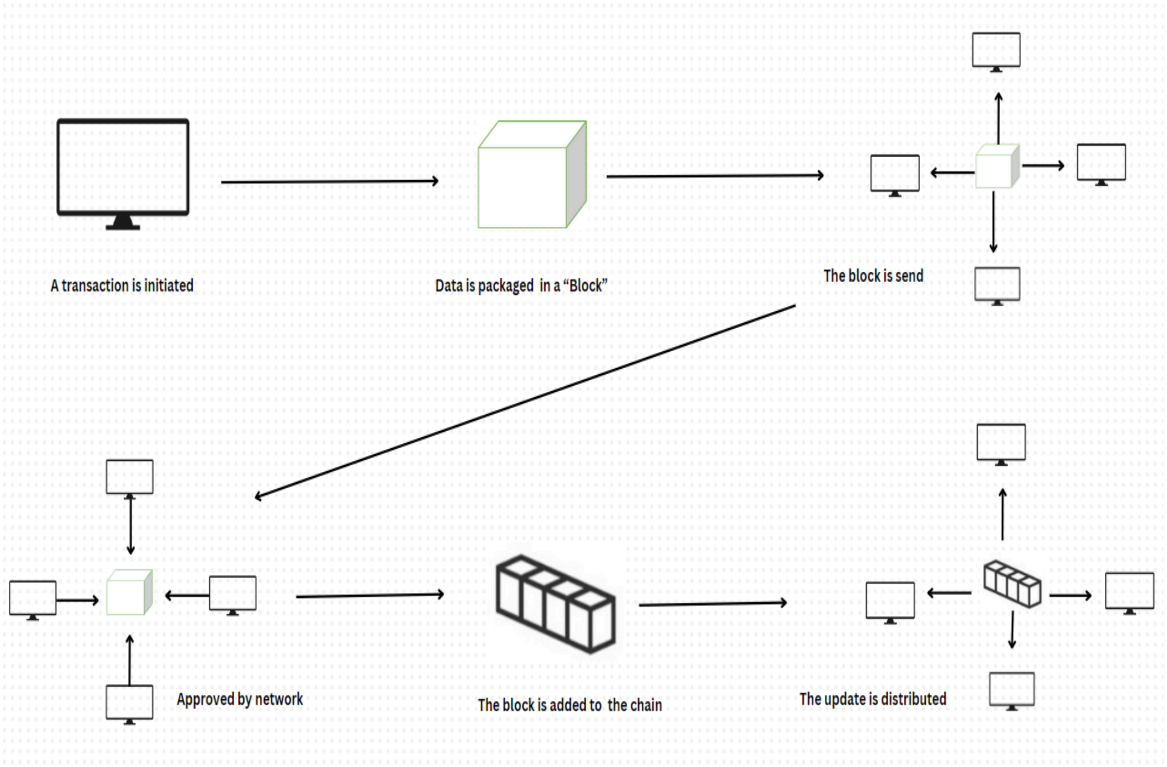

A transaction is initiated
Data is packaged in a "Block"
The block is send
Approved by network
The block is added to the chain
The update is distributed

Fig 1: How Blockchain works

Industrial implications of blockchain:

1. **Singapore's Smart Nation project:**

   The Smart Nation thinking in Singapore is the country's national aim to create a future that provides better living conditions of the residents and people across all classes. We have individuals, businesses, and government at the same table. This project starts from digital identity and gradually moves on to use IoT sensors so that public services could be automated and optimized.

   To Singapore, the force of technology empowers people to connect and be more close to their hearts, when hearts truly matter. It is using all the technologies, networks and big data that it has and is always looking for innovations through the regulator sandboxes and active recruitment; it also gives incentives to the talent through the ecosystems and the support to the startups.

In Singapore, this has been made much easier due to that it is a country with a single-tier government. It quickly works out the network of a cohesive set of working bodies. Smart Nation is a perfect instance of this principle that, usually, we have to have new technical solutions instead of politics as usual.

2. **Estonia's e-Residency:**

   Estonia brought in digital ID cards for the companies that wanted to be using the interactive services and was the first to create an e-Residency, a digital identity that was open to anyone in the world to become an online operator. However, to have a digital Estonian ID card does not mean that you automatically become a national, it only guarantees a load of benefits to an individual.

   It perfectly fit into the single-window principle which means that it is one access point and a single point of entry for citizens. The single-window principle is the mainpoint of the provisioning services like TAS and customs services for the citizens which they can get over the internet in the secure session anywhere in the world.

   The time spent in queues of banks for people of Estonia can be omitted as payslips and taxes can be done online in mere minutes. The Estonian population was helped by a tax liability calculator that got the data from the citizens' bank system. The next and most crucial plan is "corelessing" the blockchain cloud. Estonia along with Ericsson, Apcera, and Guardtime provide the development and operations of the hybrid cloud that is aimed at improving the tax reporting systems and e-health consultation with scalability and data protection capability. Nasdaq is in the process of establishing its blockchain services in the Baltic region as well. However, this issue of blockchain notarization causing difficulties in the legal system of Estonia, as well as in other countries, may be solved by blockchain providing an opportunity to verify the authenticity of documents.

3. **Better notarization in China:**

   China harbors this passion-repulsion with cryptocurrency. On the other hand, the Chinese people have been trying to clean their money out of the country or to hide the profits from taxation by using tokens. This measure has also brought strict governance from Chinese government on the use of cryptocurrencies. Yet, subsequently, the range of practical applications of the blockchain technology has been increasing, and China has been moved to the adoption of this technology for wider use.

   A good example of its early application was the company named Ancun Zhengxin Co. that was leading the transformation to the electronic data notarization services in China through partnerships with more than 100 traditional notarial offices in 28 provinces. In addition, it is providing e-data storage and electronic documents with blockchain notarization through the conventional offices.

   Ancun records thousands of data in their public blockchain using cryptography and thus, allowing the user to check the authenticity and date of notarized contracts. Most of the startups in the US are working on the same concepts. For example, Tierion.

1.2 PROBLEM STATEMENT:

During September 2021, the Indian election could have voter participation ranging from democracy, regions, and many other aspects. Voter turnouts are usually high in general elections approximately two-thirds – about 60–70 percent; the other 40–30 percent do not even turn out to the polls. The need for this stems from the desire to enhance the democratic process through electronic voting in today's digital age – inclusive, efficient, and accessible. Traditional voting methods, however, face the same hindrances that an e-voting system can beat out. Firstly, a significant factor in citizen mobility contributes to a low voter turnout in designated polling stations. Many find themselves time-bound due to work obligations or travel geographic distances. For example, this is especially true for a large multinational state such as India areas lacking accessibility like remote or rural places. An e-voting system addresses this barrier through the allowance of citizens' votes cast away while in transit or residing in distant places. They serve as barriers and may increase total turnout among voters. Secondly, an e-voting system will help in fastening the vote-counting process thus reducing the time required for outcome declaration. This prompt action reduces uncertainty, avoids protracted tensions, and consolidates public confidence in the democratic process. Finally, it may lead to higher chances of voter participation significant. They might be more willing if the target audience is more comfortable with technology voting using a digital platform. This is a fresh impetus for democratization including minority voters and voicing citizen opinions. For a successful voting process whereby all the stakeholders will have confidence in a reliable and trustworthy voting procedure, the system of e-voting has to maintain secrecy and integrity.

Election integrity is so since he or she should not in any form put themselves in a dangerous situation just for convenience. It should do so to prevent unauthorized access, hacking, and so on. In the literal sense, security measures should go hand-in-hand whenever vote manipulation is rampant. Increasing public trust is crucial. However, certain problems arise as a result of e-voting systems utilization. Preservation of voter secrecy/anonymity, protection against cyber threats, and safeguarding voters' privacy, and manipulation are critical considerations. It includes a wide range of laws and regulations. It means that we must constantly inform members of the public on how to control the e-voting process educating citizens on the security aspects involved including familiarizing them with the system, its benefits, and involvements of the society. One major while e-voting can powerless people with absentee voters due to their home location constraints. E-voting allows voters in any Internet-connected location. Some sections are inclusive in the democracy of the voting system population that was previously voteless. It can greatly affect elections. End-points supporting democracy in representation. The e-voting system must also be successful and thus credible and secure. Election integrity is because such a person should not be put in harm's way even for their convenience. It should be so to avoid any trespassing or hacking, and, in their strictest sense, appropriate security measures must prevail whenever vote maneuvering looms. Increasing public trust is crucial.

1.3 OBJECTIVES:

1.3.1. Voter Anonymity: E-voting based on blockchain can offer an equilibrium towards transparency and voter privacy. Although the voters in the booth are visible, individual voters are not anonymous. The anonymity afforded to the voters keeps them safe from fraud.

1.3.2. Fraud Prevention: The essential elements in blockchain technology. Therefore, makes it very difficult for malicious people to falsify, as well as tamper with the results. This reduces fraud It helps in enhancing the total quality of the election.

1.3.3. Reduces costs: The initial set-up costs will however run high but these are overshadowed by the gains in the long run. The adoption of a digital-based e-voting system may also help cut down the cost of printing transportation and manual vote counting.

1.4 SIGNIFICANCE AND MOTIVATION:

A secure e-voting system holds significant value in the following aspects:

- **Immutable Records:** Votes cannot be changed in the blockchain and that is why one can neither alter nor overturn them, they cannot be deleted or changed and this ensures a true voting record.

- **Global Participation:** It could be proved through an electronic voting system built on blockchains. It allows one to vote safely in any part of the world making the voting board diversified and engaging.

- **Ensuring Fairness:** The system also has a mechanism where every vote is traceable and hence verifiable. Blockchain is also made transparent and immutable as well which gives an additional boost of trust and confidence in the electoral process.

1.5 ORGANIZATION OF PROJECT REPORT:

This report is divided into 6 chapters:

i. Chapter 1 covered the introduction and central idea of the project design. The goals and techniques of the project are included in this chapter.

ii. Chapter 2 provides a review of the literature, which includes several scholarly articles on e-voting systems that we used to compare our results with those of other researchers.

iii Chapter 3 covered the system development, code snippets, and algorithms, hardware and software configuration, front-end and back-end system capabilities.

iv. Chapter 4 offers an explanation of testing resources and techniques along with illustrations of testing.

v. Chapter 5 covers the presentation and interpretation of the data in addition to the results and evaluations.

vi. Chapter 6 covers the project's outcome and future scope are outlined.

CHAPTER 2: LITERATURE SURVEY

2.1 OVERVIEW OF RELEVANT LITERATURE:

The overview of 10 research papers that are blockchain-based e-voting systems reveals the technology integration, security, transparency, and usability aspects among others. These papers as a whole, improve the ongoing talk about the electoral process reformation by the use of technological advancements.

The set of articles deals with the way blockchain is used to resolve issues related to the election of voters by traditional electronic systems. It is an essential part of this process that transparency, security, as well as decentralization, are known to be crucial. The feature that stands out and at which the ballot privacy, verifiability, and coercion-resistance occupy a place is of utmost importance for letting the voting process be complete and reliable[1][2]. The research highlights the importance of blockchain as a means of addressing some of the risks that threaten fair elections, among them – vote rigging and election manipulation - which in turn increases the confidence of the stakeholders[3]. Among the others, a paper incites the technical aspects of implementing blockchain-based e-voting systems[4]. They talk about architectural components, data management methods, and other aspects of system security that are essential for building exemplary and safe platforms. Through the application of blockchain technology's immutability and cryptographic approaches, systems strive to protect the confidentiality and integrity of voters' data while maintaining transparency and the capacity for audit of elections[4][5]. Furthermore, a paper stresses the ability to feed machine learning models into intrusion detection systems which brings about a stronger defense for this system[5]. Some papers mention blockchain democratization is the function of the governing election. They contend that through the process of decentralization and ensuring that information is transparent, blockchain-backed e-voting systems can enable voters while minimizing the threats posed by central authorities. This supports fairness, transparency, and accountability in the electoral process. Manipulation of data and bias are some of the issues addressed[6][7]. Few of the papers concentrate on operational and user capability aspects of e-voting systems based on blockchain. They revealed that user experience, system dependability, and scalability are among the indispensable factors that can be used to increase adoption and appeal. Through the utilization of distributed ledger technology and cryptographic mechanisms that blockchain offers, such systems intend to supply trustworthy, transparent, and user-friendly platforms for conducting elections[8][9]. Furthermore, they also state that smart contracts do the process of election automating and streamlining and therefore enhance accuracy and efficiency[8]. Lastly, a paper considers the socio-political impacts of blockchain-based e-voting systems, specifically in the case of underdeveloped countries. They debate the issues and successes of blockchain implementation in various electoral frameworks, underscoring the importance of an adequate governance structure and stakeholder engagement[10]. The mentioned papers highlight the capacity for blockchain not only to add transparency, accountability, and inclusiveness but to also present a new resilient and democratic electoral system.

The literature review gives a better understanding of how blockchain technology might help solve long-standing electoral governance problems. Thanks to their unique technical solutions and interdisciplinary teams, these systems are designed to support the ideas of trust, transparency, and integrity in elections which ultimately shall lead to the promotion of democratic values.

2.2 KEY GAPS IN LITERATURE:

From the analysis of ten articles addressing blockchain-powered electronic voting systems, some serious gaps, as well as issues, were detected within the context of the literature review. The matter that has been noticed is that almost all the papers have insufficient real-world application ideas. They offer numerous instructions and advice, though nothing is derived from results brought by real-life experiments and applications. It becomes tougher to gauge the viability, scalability, and acceptability of the virtual blockchain e-voting system as compared to real-life conditions [1][3]. Coming to scalability in many research papers proves to be the focal concern. The computational complexity and data storage make it more difficult to organize the distributed ledger such that the distributed ledger is applicable to big-scale elections in the system[2]. Besides, issues of scalability of consensus mechanism and transaction processing speed are still challenging enough to be expected, so it is better to keep in mind the timely and effective decision-making while solving problems[5]. Vulnerability in the security context is another important gap in the literature. Security issues such as encryption and consensus protocols are brought out in the articles, yet the possible weaknesses that can arise in blockchain systems are never talked about. In the realm of vulnerabilities, 51% of attacks, and smart contract vulnerabilities represent serious threats to the system's privacy and security, but there is no profound talk about the methods of preventing these kinds of attacks[4]. Accessibility and usability difficulties are again another significant deal in which the papers consider it. As a rule, most of the literary works are meaningless to day implementation plan. Besides, they provide lots of instructions and advice which come from imaginative data, but not science-based data from practice or experience [6]. The lack of information about the viability and scalability of using the method, and how the e-voting system now which is based on the blockchain can function in reality is a great problem[9]. Most papers were on the scalability issue. This is mainly brought about by the complicated nature of computers where accessibility might be required because of the partitioning of the ledger network and the storage of huge amounts of data during the elections[7][8]. These misfortunes are the result of the different levels of digital literacy of people living in different socioeconomic aspects and the technological infrastructures that sometimes the inequalities in voter participation or inclusiveness[10].

These matters must be talked about including digital rights, data privacy, algorithmic bias, and socio-political inequalities while ensuring that the possible negative aspects are well considered as the blockchain handles the electioneering processes. The papers have provided a strong justification for the plot but this plan shall also need the attention paid to those gaps and limitations.

Table 1: Table of Literature Survey

S.NO	PAPER TITLE	JOURNAL /CONFERENCE	TOOLS/TECHNIQUES	RESULTS	LIMITATIONS
1.	Online E-Voting System Using Blockchain Technology [1]	Ijraset Journal (2023)	Blockchain technology, Machine learning models like Gaussian Vector, Support Machine and Linear Vector.	Machine learning algorithms, which include SVM linear and SVM with Coarse Gaussian algorithms, are being used for intrusion detection in e-voting systems. SVM linear has better accuracy.	Having insufficient discussion on the possible countermeasures that can be discovered against detected attacks in e-voting systems.
2.	Secure E-Voting System using Blockchain Technology [2]	Ijraset Journal (2023)	Blockchain technology Homomorphic encryption Paillier cryptosystem	Compared to ElGamaland RSA, Paillier encryption encrypts at faster rate.	Problems associated with non-existence or poor implementation of actual-world testing for scalability and security.
3.	E -Voting System using Blockchain [3]	GCAT (2023)	Blockchain technology, E-Voting system development, Security measures for fraud reduction and mobility enhancement in voting processes.	Paper on an electronic voting system based on blockchain serves to discourage fraud, maintain fairness, and simplify voting.	Poorly explained technical details in blockchain-based e-voting systems can minimize public understanding of their operation by certain groups, hence leading to reluctance to use them.

4.	E-voting System Using Block-Chain [4]	Ijraset Journal (2022)	Blockchain technology, Merkel trees Cryptographic foundations, Multi-factor authentication, Encryption and Digital signatures	The application of blockchain in e-voting prevents any leaks, and ensures the public nature and fairness of the digital voting process.	Problems that come up during the process like scalability, interoperability, and availability of the citizen to the system are some of the areas that need to be properly addressed if blockchain technology is to be adopted as the basis of e-voting.
5.	Design and Implementation a Smart E-Voting Model : Decentralization Using Blockchain[5]	Ijraset Journal (2019)	Decentralized Blockchain technology, Solidity language, JavaScript and Cryptography-based voting protocol design processes.	Proposed a decentralized Blockchain e-voting platform that guarantees the security of voter's ID, the confidentiality of information transfer, and the verifiability of the results.	Legal, social, technical, and security problems are the challenges in e-voting systems. a
6.	VoteChain: A Blockchain Based E-Voting System [6]	Ijraset Journal (2019)	Blockchain Technology, Central Database Comparison, Real-World Testing and Security Measures.	Blockchain-based e-voting system VoteChain proved its credibility during real elections and it proves that large-scale of transparent and secure elections can be successfully achieved using this system.	Accuracy of the outcomes of elections on VoteChain comes with exposing the cases of electoral injustice, however, there are national variations not factored in. In addition, it is possible to do a broader study of scalability problems and to decide its feasibility to use it for all types of elections.

7.	Trustworthy Electronic Voting Using Adjusted Blockchain Technology [7]	IEEE Conference (2019)	Effective hashing techniques, Block creation and block sealing concept, Consortium blockchain, Selection of suitable hash algorithms and Adjustable blockchain method	The end products are secure storage of the data, the transparent process of voting, and the flawless process of results announcement using blockchain technology.	The research has some limitations in the e-voting process, which are addressed in a separate part.
8.	An Anti-Quantum E-Voting Protocol in Blockchain With Audit Function [8]	IEEE Conference (2019)	Secret sharing, Blockchain technology, RSA encryption.	It abolishes the function of the department of pseudo-registration and the casting of the ballot in secret at the same time.	The memorandum is somewhat vague, implying that the solution is only one part of the solution and without any explanation of testing in real life or in the field.
9.	Securing e-voting based on blockchain in P2P network [9]	EURASIP Journal (2019)	Distributed Ledger Technology (DLT), Elliptic Curve Cryptography (ECC), Blockchain-based e-voting system and Linux platforms	The deployment of tangible blockchain network over Linux operating systems does not only lend extra potency to the protection scheme but also increases the privacy and anonymity in electronic voting.	Not being aware of the scalability options and the unconscious risks that will be implemented into the created blockchain system of electronic voting.

10.	Maintaining Voting Integrity using Blockchain [10]	ICECCO Journal (2019)	Blockchain technology. Distributed ledgers, E-voting protocols, Integrity requirements for online and offline voting and Framework conditions for blockchain-based voting	To highlight fluctuations in the price of cryptocurrencies, the challenges of e-voting protocols, as well as security in online and offline voting, blockchain needs to assimilate the concept of integrity.	It is not likely to use only blockchain technologies to build the ene-voting system with ignoring the other available technologies at the same time. Whereas this is quite an advancement, obstacles that could be faced during such a process are ignored in the research.

CHAPTER 3: SYSTEM DEPLOYMENT

3.1 REQUIREMENT AND ANALYSIS

3.1.1 FUNCTIONAL REQUIREMENTS

Functional needs of a safe E-Voting platform based on blockchain include significant operations processes and competencies that should be put into consideration during a good day-to-day running of the company. These include:

1. Voter Authentication:

- Putting an efficient voter identity system in place will only permit authentic
voters to access polling stations through it.

2. Vote Casting:

- So that each eligible voter's ballot is securely placed inside the box.

3. Immutable Ledger:

- Using Blockchain technology so that nobody can change it, and thereby maintain
an honest and secure system.

4. Privacy Preservation:

- Privacy of voters should be ensured.
- Ensuring that the elections are conducted in an honest manner.

5. Results Tallying:

- They will be able to record the votes, they can then automatically tally and
aggregate these votes.

6. Auditing and Transparency:

- Ensure transparency by subjecting the node to the blockchain.
- Ensure that proper stakeholders can trace the integrity of the elections.

7. User Interface:

- An interface for e-voting can be prepared for the voters in advance.

3.1.2 NON FUNCTIONAL REQUIREMENTS

In some cases, performance characteristics could be extended as a kind of non-functional requirements. However, it is not possible to define such an attitude toward all performance criteria security, and usability of the e-voting system:

1. Security:

- For example, security-enhancing (encryption, secure key manager).

2. Scalability:

- Be sure you can handle several things simultaneously.

3. Usability:

- Making it easier for non–technical people to traverse and find, rather than getting lost.

4. Reliability:

- Ensure that it does not move by giving it a stronger arrangement.

5. Performance:

- Create a system that will redesign the existing system to cut down latencies and delays in voting.

6. Accessibility:

- A free system, however, should include the perspective of the blind who cannot vote by themselves and only in absentia through other persons incorporating inclusive design principles.

3.1.3 System Constraints

System constraints refer to the limitations and conditions that have to be followed by the e-voting system within:

1. Regulatory Compliance:

- Ensure that the online voting mechanism is also in conformance with all relevant laws as well as regulations.

2. Technology Compatibility:

- Evaluate if it fits in well with already established infrastructure, and works alongside other systems, and any IT personnel implications.

3. Resource Limitations:

- Identify resource limits such as low bandwidth as well as processor power.

4. Budgetary Constraints:

- The implementation of the e-voting system under budget restrictions.

5. Geographic Considerations:

- Consider the potential differences as far as a voter is distributed according to geography and the variability of the Internet.

6. Data Privacy:

- Comply with strict data privacy standards meant for the voters.

3.2 Project Design and Architecture

Architecture:

1. User Interface (UI):

- It's the user interface that acts as a medium of communication between the system and its users. Task-based, but with a visually intuitive user interface verifying voters, electing ballots, and casting votes. The design prioritises ensure that they have included voter experience to cater for voters at different levels of technical competency.

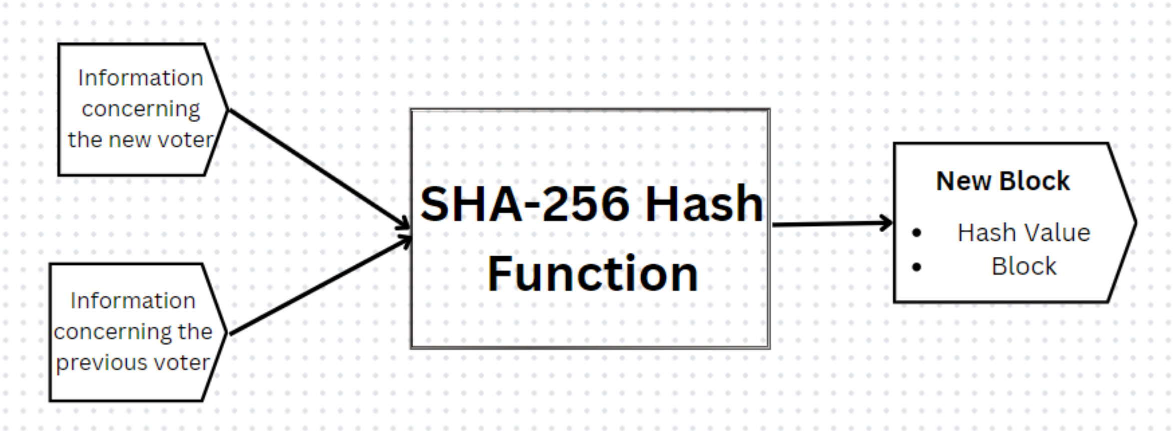

Information concerning the new voter
Information concerning the previous voter
SHA-256 Hash Function
New Block
Hash Value
Block

Fig 2: Creation of a new Block which contains Hash value and Vote.

2. Voter Authentication Module:

- These are the requirements that this module aims to establish during voter verification prior to giving access to the e-voting system. Such includes the use of sophisticated authorization techniques like two-factor authentication. For higher securities, to include measures like multi-factor authentication or biometric verification. The voting process should be managed by an independent party to ensure all genuine voters are counted.

3. Blockchain Layer:

Every node on the blockchain network has an identical copy of the blockchain shown in where every blockchain is a collection of transactions.The blockchain stores tamper evident, encrypted voting records. This ledger acts as a permanent and transparent audit trail for all ballots cast and preventing fraudulent activities.This enhances transparency and accountability, adding further dimension to check on the genuineness of the whole voting process.

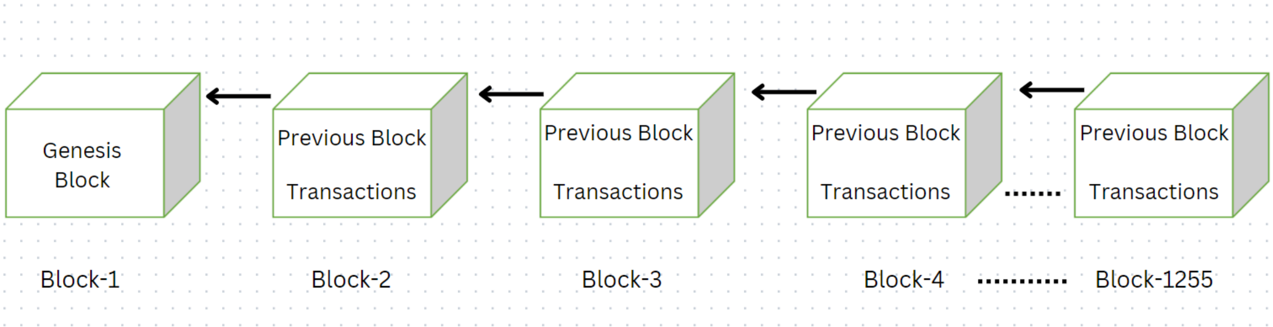


Fig 3: Blockchain data structure

4. Privacy-Preserving Module:

SHA-256 is one of the high-end techniques that have been included in this module voter certification schemes which are designed to ensure that votes cannot be traced to voters' voting process. It protects specific voting options and aggregates them together for verification of overall results.

5. Security Layer:

This layer safeguards the integrity. It plays a crucial role in ensuring the safety of the e-voting system by averting access and alteration from unwanted sources.

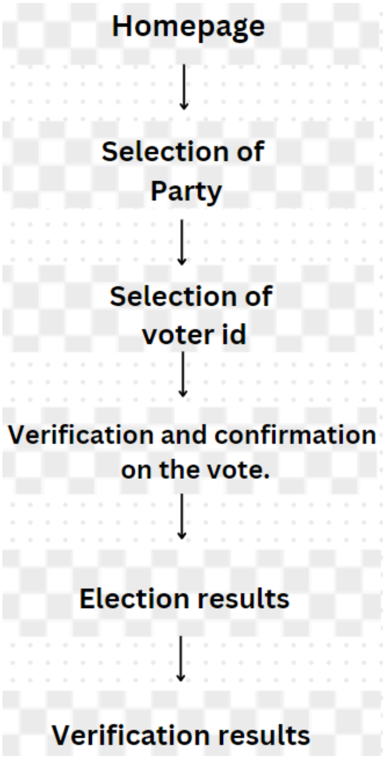


Fig 4: Layout of e-voting system

3.3 Implementation

3.3.1. Blockchain

Bitcoin, the first and most well-known example of the use of blockchain software, has been quietly arriving in the blockchain technology movement since 2009. Furthermore, the Bitcoin creator remained anonymous, but an alias called Satoshi Nakamoto was left behind.

"Bitcoin makes Blockchain, and email builds the internet," writes Sally Davies of the Financial Times.

With just one currency, the developer of Bitcoin software is aided by a massive electronic system. Soon after, in 2014, it was revealed that blockchain technology can be used by organizations rather than cryptocurrency exchanges. Nonetheless, several individuals felt that both Bitcoin and blockchain were the same throughout 2018. The aim of blockchain technologies is to redefine the system's "confidence" that replaces intermediaries such as governments and companies, i.e., the framework of the next generations, decentralization. With blockchain technologies, instead of intermediaries that are responsible for both data protection and stability, the 'trust' would be on the framework or so-called smart code.

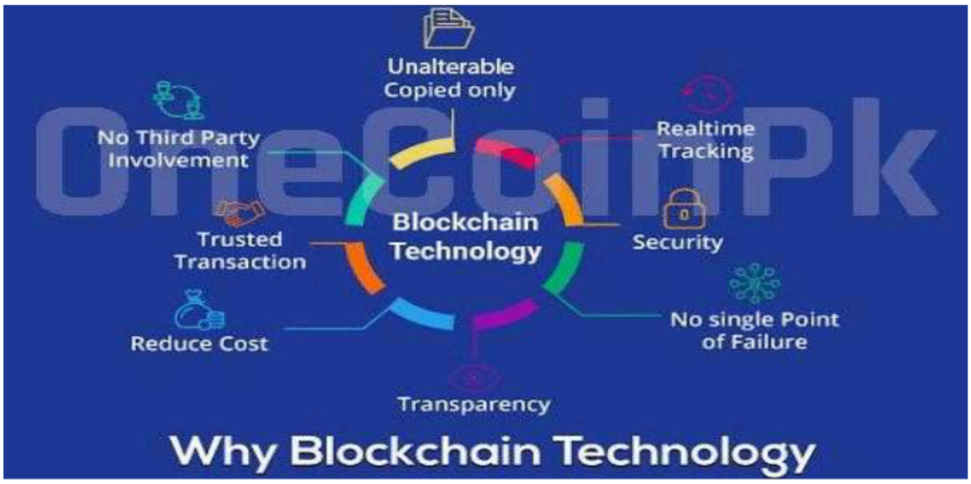


Fig 5: Blockchain Capability [13]

Blockchain technology skills, however are what inevitably require clarity, immutability, and so on in the e-voting system (Fig 5). Currently numerous forms of blockchain, and the new so-called "smart contracts" breakthrough have been established.

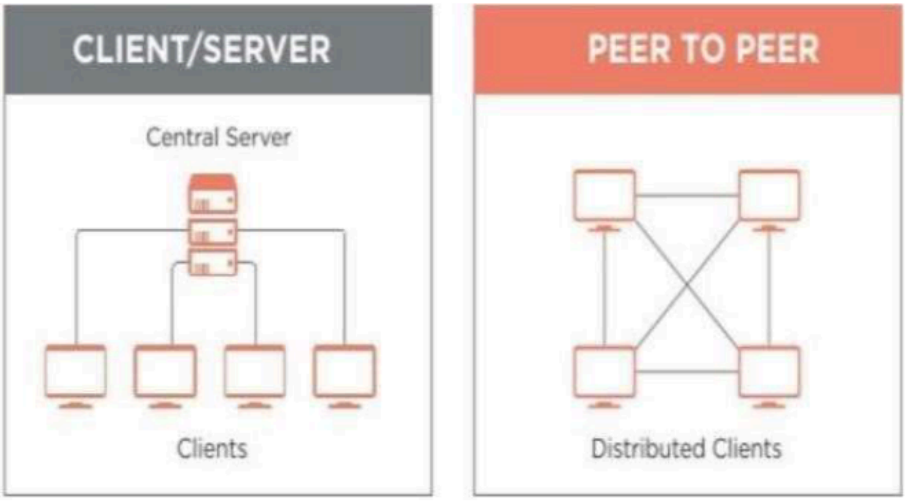
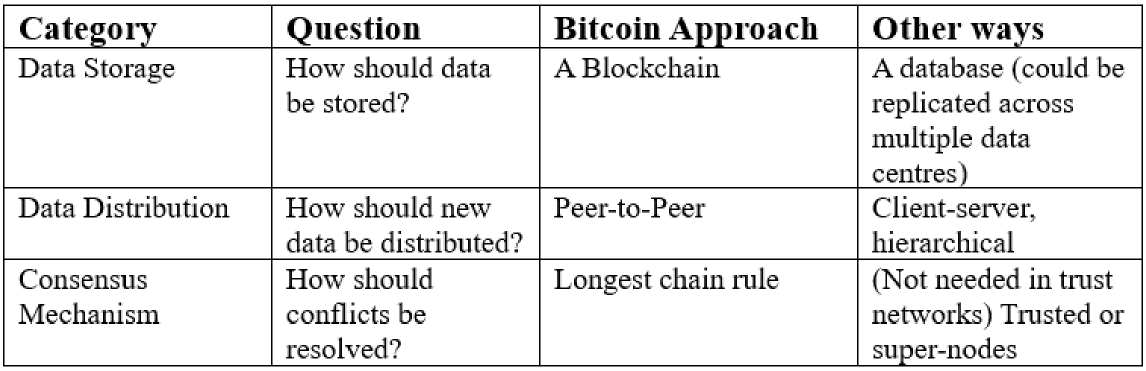


Fig 6: Centralization vs. Decentralization Architecture [14]

In the case of centralization, a server occupies dominant power whereas the client occupies minimal power. As we can see Fig 6 depicts that, in case of decentralized architectures, the scale of the authority is full. Theoretically, blockchain. Currently, it is a peer-to-peer community in that each node represents a single part of the system, though more than one. Finally, ‘its nearest approximation in this factor,” meaning support for the network at the level of each stage.

Table 2: Table of Difference of dApps and Centralized Apps [14]



Category	**Question**	**Bitcoin Approach**	**Other ways**
Data Storage	How should data be stored?	A Blockchain	A database (could be replicated across multiple data centres)
Data Distribution	How should new data be distributed?	Peer-to-Peer	Client-server, hierarchical
Consensus Mechanism	How should conflicts be resolved?	Longest chain rule	(Not needed in trust networks) Trusted or super-nodes

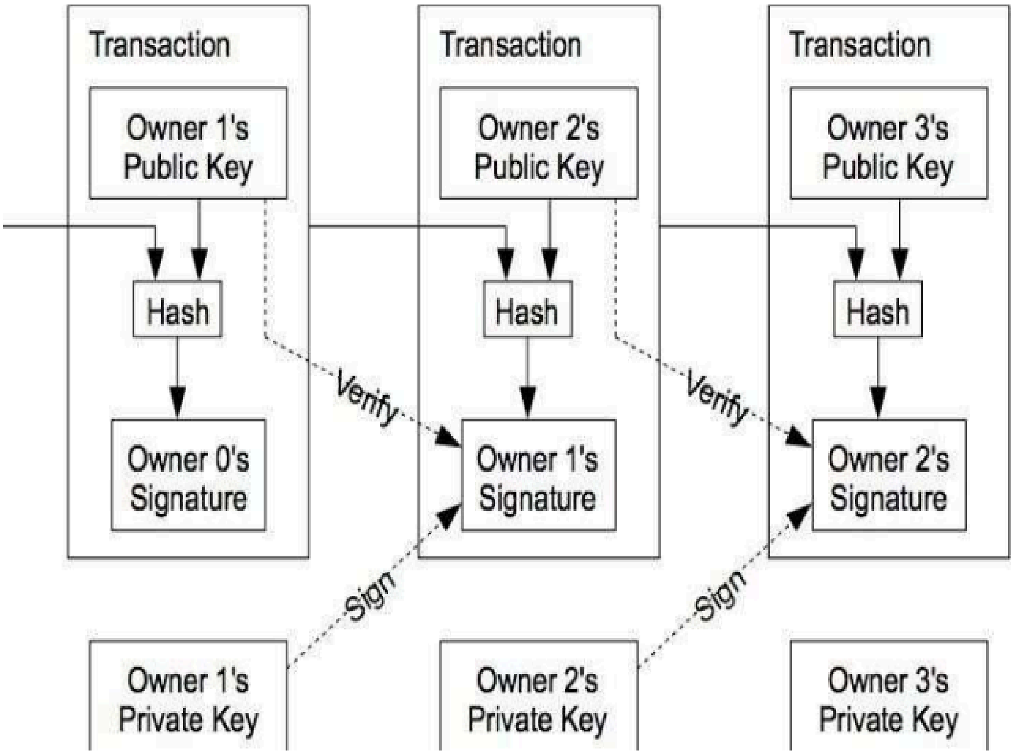


Fig 7: Cryptography Block [15]

As can be seen clearly in Table 2 the simple comparability is clearly exhibited between dApp and centralized application. In the P2P the copies are stored at each node simultaneously and synchronously distributed to blockchains. The insertion that occurs in block-chain does not necessitate any revisions done. Fig 7 shows the cryptography block.

3.3.2. Permissionless and Permissioned Blockchain

Owing to the large and diverse application styles i.e. (P2P trading and P2P freelancing), which have been generated to result in multiple forms of blockchain.The primary reason behind the scene which activates the blockchain's numerous properties.There are private ones afterward. The blockchain was found by organisations such as banks, and a permissioned blockchain arose.

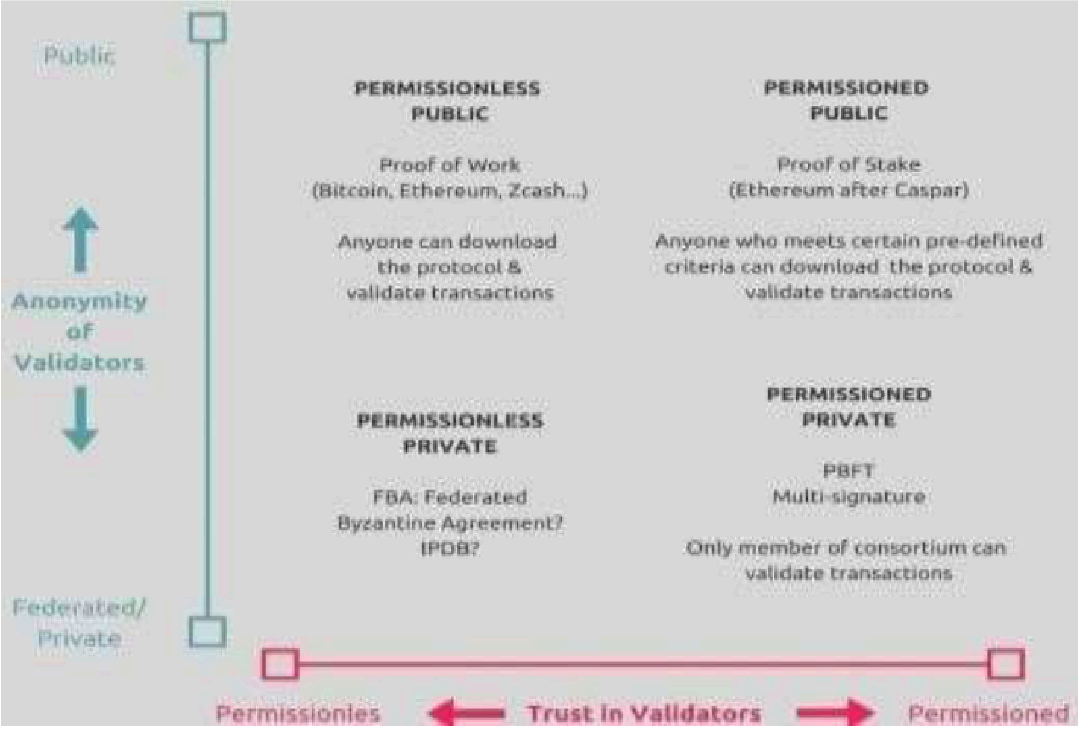

Public
PERMISSIONLESS PUBLIC
Proof of Work
(Bitcoin, Ethereum, Zcash...)
Anyone can download the protocol & validate transactions
PERMISSIONED PUBLIC
Proof of Stake
(Ethereum after Caspar)
Anyone who meets certain pre-defined criteria can download the protocol & validate transactions
Anonymity of Validators
PERMISSIONLESS PRIVATE
FBA: Federated Byzantine Agreement?
IPDB?
PERMISSIONED PRIVATE
PBFT
Multi-signature
Only member of consortium can validate transactions
Federated/ Private
Permissionles
Trust in Validators
Permissioned

Fig 8: Permissionless and Permisioned [16]

In reference to fig 8:

- Public Blockchain without authorization. Open to the public without authorization to cast and check the ballot and to display the results (FFA).
- Public approved blockchain. Limit the casting and checking of the ballot to registered electors. The suggested scheme would use the Public Permissioned Blockchain as follows, which is ideally tailored to the scenario.
- After the voting is over, the registered elector can cast and check their vote and inspect the results.
- A poll/election that requires the registered elector to join and display the results during the process can be produced by the organizer.

Public vs Private Blockchain

Access control type is used to classify blockchain for public and private blockchain. Different types of blockchains are public blockchains, which are called permissionless blockchain, and private blockchains, which are also called permissioned blockchains. The two are differentiated by way of mechanisms of obstruction to access. Public or permissionless blockchains do not appoint novel or any new nodes into the network, and simply anyone can engage the network. A central entity or a privileged group of members controls private blockchains; their network is small and there is a limited number of nodes in the network and not everyone can join the network. Blockchains that are open to all individuals are public blockchain which are Bitcoin and Ethereum main nets. One can see private chain (blockchain) such as small Ethereum network where few nodes are connected to each other and thereafter not connected to any other main network. The nodes of the network will connect to form a private blockchain.

Organised blockchain network is mostly employed by large enterprises for the sake of data exchange with its partners and/or subsidiary agencies.

It is worth noticing that in developing applications for blockchain the type of blockchain you choose will be the determinant for the rules of engagement with the blockchain to either be same or non-conforming. The-public has predefined set of rules and a the-private can have different rules of the-blockchain per blockchain. As for a customer-oriented supply-chain, a private blockchain may have different governance regulations, while a public blockchain set for protocol governance may be based on different set rules. For instance, currencies, gas fees, transaction fee, endpoints, as they went into the main net may not be the same as what they had in the main net.

3.3.2 Structure of Blockchain

Through the process of mining,every new transaction is grouped into blocks that contain all the data from a set of past transactions. Every node on the blockchain network has an identical copy of the blockchain,where every blockchain is a collection of these blocks that contain the data from these past transactions. There are two parts which make every block that much complete. 'The header' part is like a head in the chain so it links back to the previous block. This is the answer for the question - What does it mean that every block header stores the hash of the previous block; no one can alter any transaction in the previous block, might be the answer that occurs to your mind. The other section of the block is about 'body content' and has a bullet proof list of transactions, their amounts, the addresses of the parties, and some supplementary data. Thus, the way a particular block immediately follows the previous block makes it possible to look at all the preceding blocks in a blockchain. Irreversibility and immutability are the features in blockchain transactions. These allow no modifications in transactions. Every time the units are changed, the information which is to be verified by the collaborating nodes gets moved to new transactions. Each of the nodes consisting of the blockchain has a separate copy of blockchain.

3.3.3 Digital fingerprints to the blocks

The ciphering part of the blockchain is the most important one among others. It is the way to keep the details secret, avoiding any vulnerabilities by using encryption methods. It ensures confidentiality,integrity of data,authentication,non repudiation etc. Since it is just a text of message,numerical data or any program which a computer can execute,the plaintext is the name for it. The purpose is to apply an encryption algorithm to the plaintext to perform encryption. Higher the quality of algorithm, the less chance of an adversary on the way. Cryptographic hashes, the functions, are generally considered the most important tools and are an integral part of the blockchain data structures. One of the key cryptographic techniques employed in a cryptocurrency is public key cryptography, which is at the heart of many the cryptographic protocols. Cryptographic hashes are the certain kind of hash functions that are perfect for cryptography sensing. Now, a Cryptographic Hash Function is a one-way as well as a deterministic function which converts arbitrarily long input data to fixed output length. Output is imprinted into “hash value” or “message digest” subsequently. SHA is thorough to mean the secure hash algorithm. This version is the latter of the SHA-2 family. SHA-256 is a family primitive hash function and other variants are its derivatives. SHA-256 yield objects with 256-bit lengths. Furthermore, SHA-256 applied to 32 bit word and SHA-256 uses Merkle-Damgard construction.

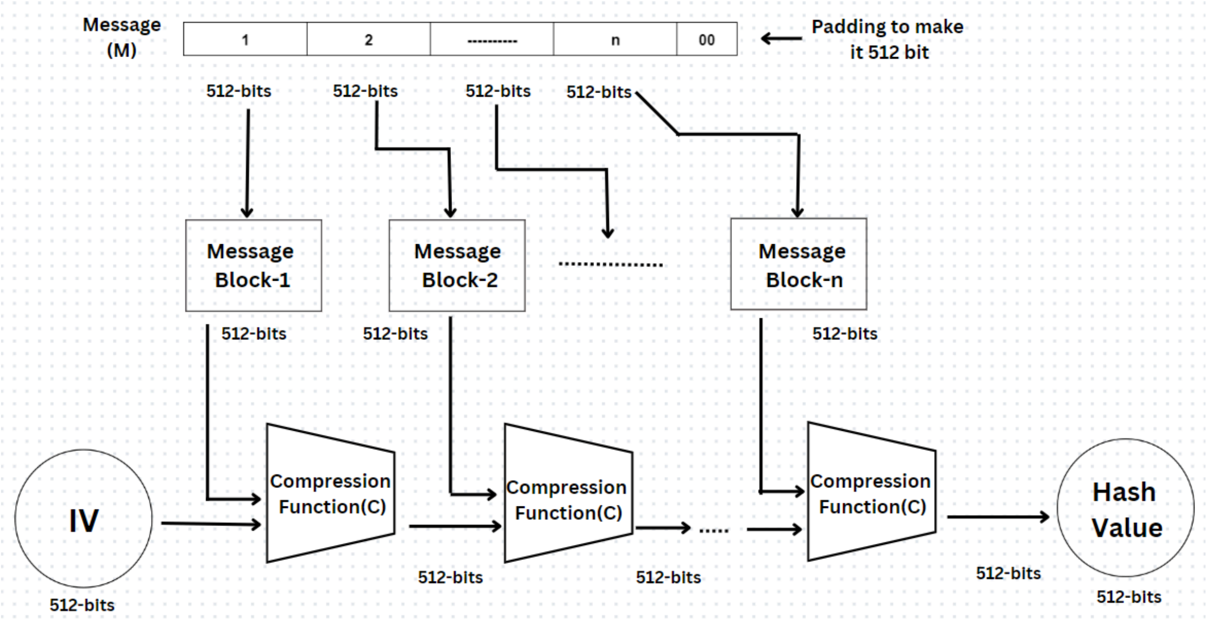


Fig 9: Merkle-Damgard construction for SHA-256.

3.3.4 Chain the blocks

The term “blockchain” means “the blockchain data structure,” which is, after all, a chain of blocks linked together. "Blockchain" when said, the word means either one single transaction or a whole group of transactions. A simplified substance that resembles the component of linker is a hash pointer. A hash pointer is a cryptographic hash of the data block,wherein the hash pointer is a reflection of the data block itself. As hash pointer points to the previous data block and due to this, an ability to verify that data has not been replaced is created. Hash pointers primary role is to allow for a trusted blockchain that can be regarded as one of the possible sources of the truth. The hash of the prior block is contained in the current block header. In the same manner, the hash of the current block including its block header will be stored in the header of the next block. Each block links them to the previous block or parent block. Once the new block is being confirmed to the chain, it becomes a parent block to the next go. The chain of blocks relies on the first block to tie them all together, that is called the "genesis block". In this regard, data is practically impossible to alter at any time as no one can change the information in any of the blocks. In this case, the block hash will be created by SHA-256 and it will output 256 bits of hash.

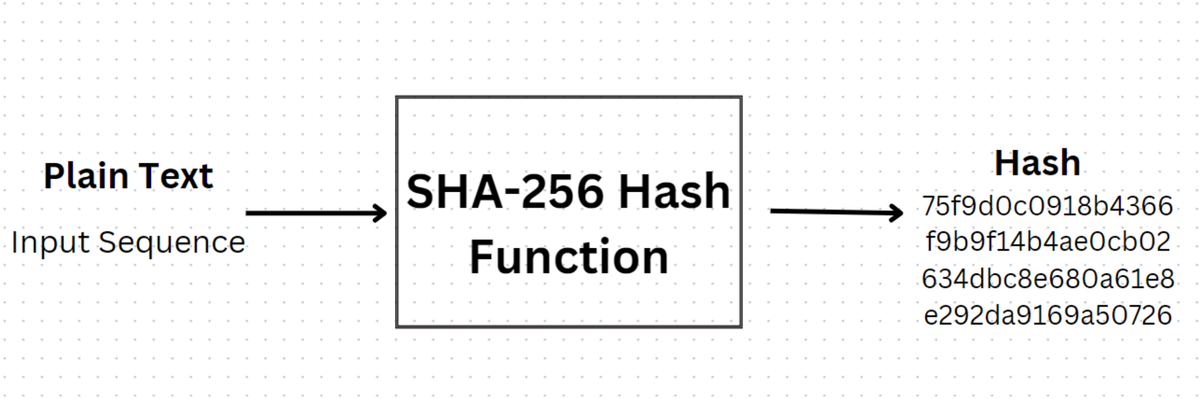


Fig 10: Basic Function of the SHA-256 Hash.

3.3.5. Transaction

A transaction is a collection of instructions for changing the blockchain's state. In order for transactions to be processed by specialised nodes, or so-called miners, and confirmed by the network, transaction fees are a feature of public blockchain networks (See 2.1.4). Miners put forth a good show. For a monetary incentive, you must perform computational effort. For the following reason, it is important to briefly present Unspent Transaction Outputs in order to truly comprehend what a blockchain state is.

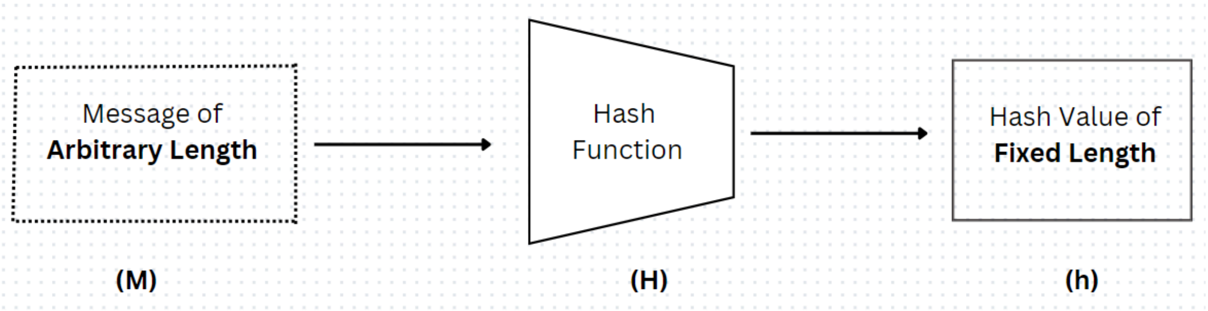
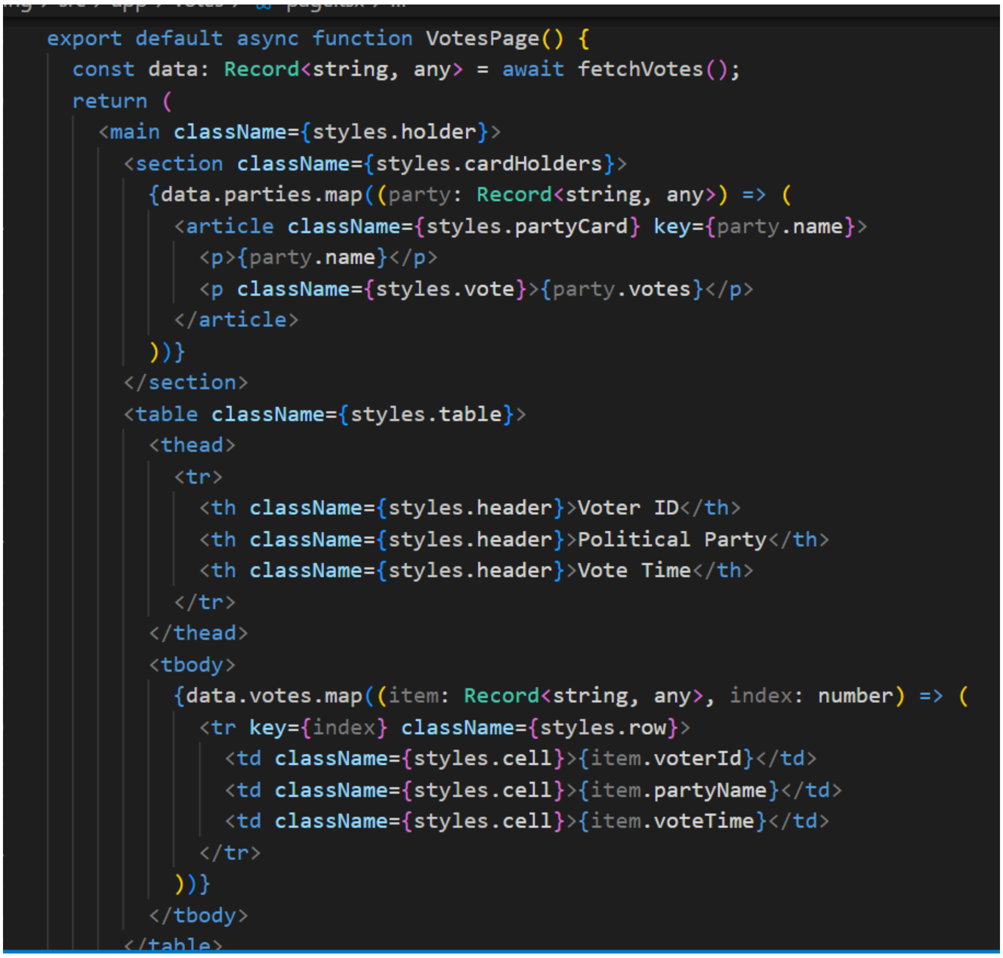


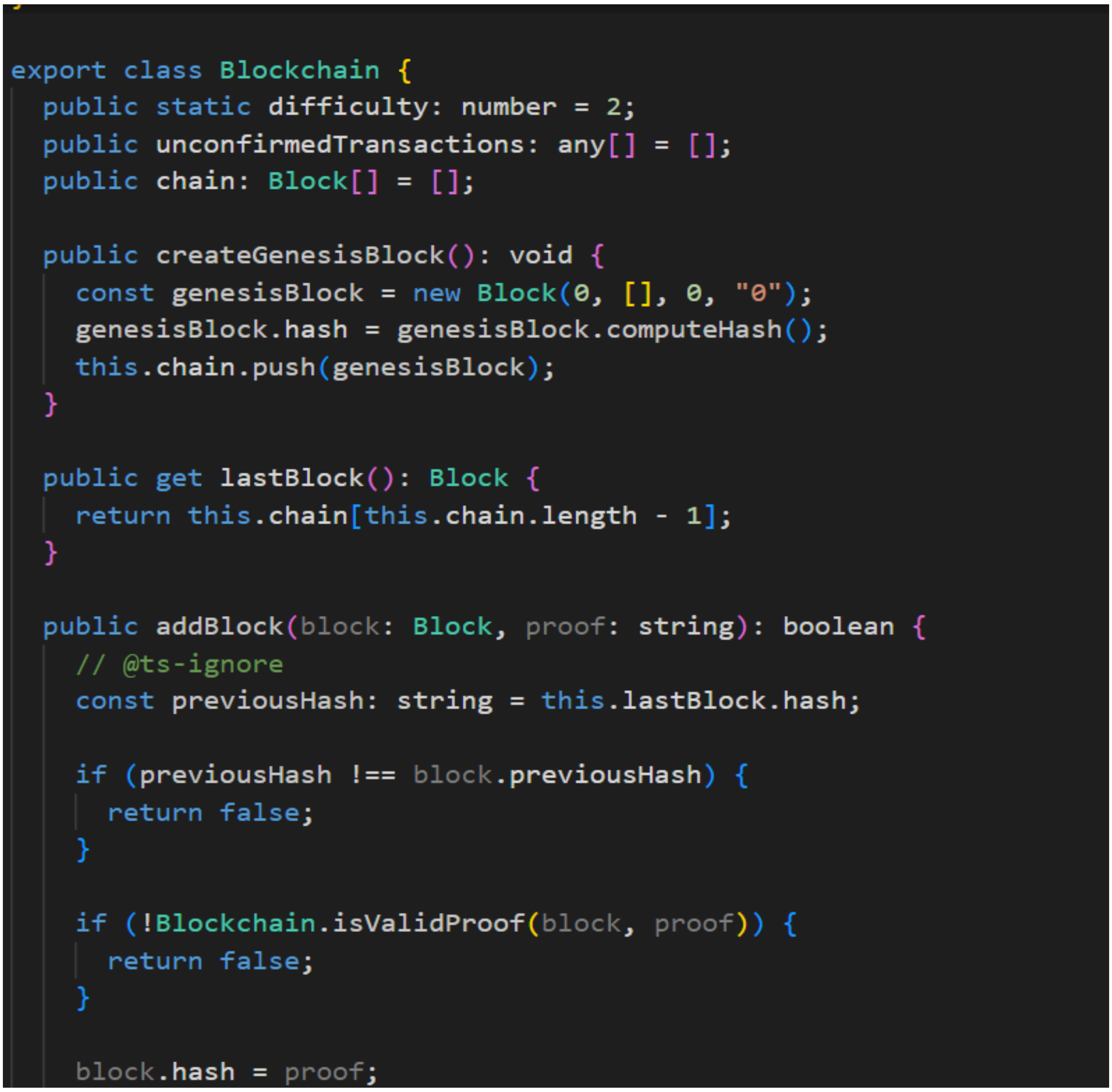
Fig 11: Basic form of Hash Function.

Code snippets:



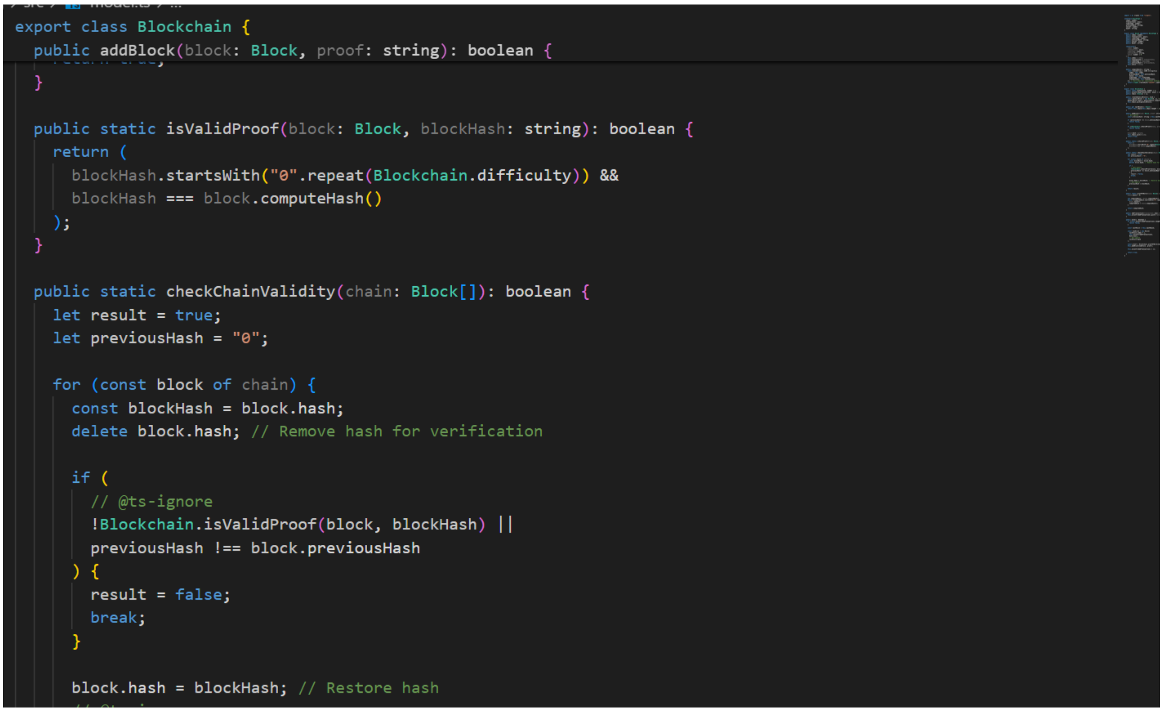
```
export default async function VotesPage() {
  const data: Record<string, any> = await fetchVotes();
  return (
    <main className={styles.holder}>
      <section className={styles.cardHolders}>
        {data.parties.map((party: Record<string, any>) => (
          <article className={styles.partyCard} key={party.name}>
            <p>{party.name}</p>
            <p className={styles.vote}>{party.votes}</p>
          </article>
        ))}
      </section>
      <table className={styles.table}>
        <thead>
          <tr>
            <th className={styles.header}>Voter ID</th>
            <th className={styles.header}>Political Party</th>
            <th className={styles.header}>Vote Time</th>
          </tr>
        </thead>
        <tbody>
          {data.votes.map((item: Record<string, any>, index: number) => (
            <tr key={index} className={styles.row}>
              <td className={styles.cell}>{item.voterId}</td>
              <td className={styles.cell}>{item.partyName}</td>
              <td className={styles.cell}>{item.voteTime}</td>
            </tr>
          ))}
        </tbody>
      </table>
```

Fig 12: Votespage function



```
export class Blockchain {
  public static difficulty: number = 2;
  public unconfirmedTransactions: any[] = [];
  public chain: Block[] = [];

  public createGenesisBlock(): void {
    const genesisBlock = new Block(0, [], 0, "0");
    genesisBlock.hash = genesisBlock.computeHash();
    this.chain.push(genesisBlock);
  }

  public get lastBlock(): Block {
    return this.chain[this.chain.length - 1];
  }

  public addBlock(block: Block, proof: string): boolean {
    // @ts-ignore
    const previousHash: string = this.lastBlock.hash;

    if (previousHash !== block.previousHash) {
      return false;
    }

    if (!Blockchain.isValidProof(block, proof)) {
      return false;
    }

    block.hash = proof;
```

Fig 13: Blockchain logic function



```
export class Blockchain {
  public addBlock(block: Block, proof: string): boolean {
  }

  public static isValidProof(block: Block, blockHash: string): boolean {
    return (
      blockHash.startsWith("0".repeat(Blockchain.difficulty)) &&
      blockHash === block.computeHash()
    );
  }

  public static checkChainValidity(chain: Block[]): boolean {
    let result = true;
    let previousHash = "0";

    for (const block of chain) {
      const blockHash = block.hash;
      delete block.hash; // Remove hash for verification

      if (
        // @ts-ignore
        !Blockchain.isValidProof(block, blockHash) ||
        previousHash !== block.previousHash
      ) {
        result = false;
        break;
      }

      block.hash = blockHash; // Restore hash
```

Fig 14: Blockchain logic function

3.4. Key Challenges

Key features in the implementation of a Secure electronic voting (e-voting) system using blockchain challenges. For starters, voter information has to be kept safely and confidential since it involves a failure to adhere to this can compromise the whole election process. Privacy-preserving effective provisions should be put in place for protecting an individual's vote. The decisions should be made in a way that do not compromise the entirety of the system. Scalability is another major this presents a great challenge in big elections that involve massive transactions processed efficiently. This is because blockchain networks such as ethereum requires novel methods of dealing with a huge volume of ballots, compromising speed and performance. Additionally, the e-voting system is integrated with working closely with existing legal and regulatory frames poses challenges to resolve these legal ambiguities and ensure compliance, it must involve some relevant authorities. Additionally, hence, consideration should be given on the user experience and accessibility of the system catering for different population groups, as well as individuals with varying levels of computer literacy.

Lastly, this requires continuous research and development of countermeasures against emerging threats such as terrorism and cybercrime vulnerability, with this being a changing environment where emerging threats could emerge every time. Overcoming these hurdles lies in getting this type of adoption off the ground on the efficiency of blockchain electronic voting system.

CHAPTER 4: TESTING

4.1 Testing Strategy

Mining

The mining operation in the Blockchain is one of the core processes that are critical for decentralized network operation security. The process implies the verification of these deals and their grouping in blocks, which are chronologically attached to the Bitcoin-chain-like structure. This validation procedure employs cryptographic mechanisms and agreements like Proof of Work (PoW) or Proof of Stake (PoS) that perform the work depending on the particular blockchain protocol.

PoW means that the miners compete to solve intractable mathematical problems, which demand massive amounts of computational capacity. This spurs the prevention of unlawful actions and monitors putting forward effort for introducing a new block in order to keep the network stable. Miners are constantly voyaged to find a hash value that will meet a certain set of criteria; this set for example may have the prerequisite of containing 32 leading zeros. Once a miner finds a correct solution it broadcasts the network to the network centers to verify the solution.

As confirmed by the following round of verifications from other participating nodes, the block created by this miner is now the additional part of the blockchain, a journal of recent activity. On top of checking the legality of these transactions, miners also have an important defensive function, protecting the network against such threats as double-spending and maintaining the general peace and harmony among participants.

Miners are earning coins as their remuneration and resources that are directly proportional to the number of blocks of the chains and service fees that are added to the transactions. This in turn encourages real engagement of the network, which consequently aids in decentralization and resistance of blockchain ecosystems against inferences.

In the world of advancement in technology, mining provides the foundation walking block for blockchain technology that enables secure, trustless, and tamperproof transactions and helps to protect network integrity. Nevertheless, with ongoing development, new consensus mechanisms and mining algorithms could appear, but the fundamental security truth and validation of transactions stay at the domes of any blockchain structure.

Set up the blockchain

Since the blockchain system by the SHA-256 hashing algorithm requires to be set up, some considerations are necessary. The primary factor to consider is choosing a blockchain platform or framework based on its capability to support custom consensus mechanisms and hashing with SHA-256 encryption.

Network configuration becomes easy when you choose a platform and take such critical actions to fine-tune the most critical network parameters. This is inclusive of-setting up the block size, block time, difficulty function target, and others that are vital for the PoW consensus mechanism. Make sure that the final parameters are fit with the abilities of SHA-256 and network features that are expected.

Second, deploy and configure nodes to function as a network node on the blockchain. Accordingly, nodes must be equipped with software that is effective at doing the per-transaction hash creation activities under SHA-256 algorithm to check transactions and mine new blocks. Look into the equipment specifications and growing factors as you make nodes so that sufficient node to handle the volume of transactions expected is there.

Design or integrate mining software that employs SHA-256 encryption for block verifying and for granting mining rewards. This application must therefore be able to work promptly in order to complete all necessary computations while respecting the network regulations and the protocols of the blockchain.

Develop and enforce stringent security controls that guard the network against susceptibility to SHA-256, related issues including hash collisions or algorithm weaknesses.This can encompass the rigorous securities audit, high-end encryption protocols, and access control systems, which can ensure the protection of the skin.

Testing the network for blockchain must be done meticulously to the point where it is guaranteed to be compatible and stable with the selected hashing algorithm. Study the ordinary operation, edge cases, and the attacks' vectors from the beginning to the end, finding the issues that might be there and resolving them.

Hashes

While the hashes are crucial and indisputable part of the blockchain technology, they have a pivotal role in blocks data security acting as blockchain unique and unquestionable fingerprints. Also, these cryptographic hash functions use a function that takes an input and produces a constant or a fixed-size output resembling with the change of the size of the input, the change of the hash value become completely different. Each block of the chain consists of a header and a transaction list containing the hash of the previous block. The common feature of the blocks is a chain that creates an ordered stream of blocks. Therefore, the link via hash makes the data uncorrupted and unchangeable, as any modifications in a prior segment would be considered as invalidation of subsequent sections. Besides, hashes are frequently utilized in proof-of-work or PoW consensus mechanisms, where miners compete to discover nonce that satisfies the difficulty goal (by means of an accepted hash value). This is a process of mining that not only offers protection for the whole network but also gives mining new blocks to the blockchain. Besides, the hashes serve a purpose for proving the integrity of transactions, authentication of the participants via digital signatures and as a result, achieve the overall environment of trustability and transparency.

A hash function can employ any size of the input data, perform an operation, and return a "hash" - a data of the fixed size. Either it is a single sentence or the Oxford Dictionary, the size of the resulting hash will always be the same.

a) Rather than being just a generic identifier, an eye color can almost be considered an individual trademark. Blocks, transactions and addresses are in fact referenced by means of hashes in the blockchain. In Bitcoin, the blockchain hashes are 256 bits or 64 characters. This algorithm used in blockchain is known as SHA-256. SHA short for Secure Hash Algorithm resulting in the generation of 256-bit hash.

b) It is one-way and hence it is a good fit for encryption. A hash function can take a string or input of any length to produce a fixed-length data output. But, we cannot directly go by the data output and make the string/input renewal.

c) Often a slightest differentiation makes a unique hashing value to occur as one of the most resistant functions.

d) It reduces the size of the database. Besides that, the space that the output takes is always going to be fixed. Henceforth, one should just store the hash of a file to the database instead of the file itself because the latter takes up more space in the database. For instance, you can hash the photo of the painting, including the details of the painter, the date and the place of the painting, and then create a hash out- put. Only the hash of the painting needs to be stored in the database where the hash serves as a mathematically computed unique identity of the original painting and data.

The resulting hash with 64 alphanumeric characters will not only make a huge number of combinations but also it is almost impossible to know the repeated one.

Next.js

Next.js is a strong tool for the process of creating apps for the web, which seeks to make it simpler and more comfortable. It delivers a harmonious couple of easy and flexibility, therefore developers can use this robust framework to create server-side generated React apps with so much ease. Serving server-side rendering and static site generation are the two inseparable built-in components in Next.js. In addition to I/O and memory functions, Javascript gives developers the opportunity to improve resources utilization and gives users the possibility to get interactive experiences on the Web. With a powerful API and a large set of plugins, editing process can be done faster and the development workflows are streamlined thus helping teams build complex applications more efficient functions, such as 'document. createElement', enable you to give life to your imagination, reliably, and as fast as possible. React along with its multiple js, a top-notch React framework, is hugely admired for its user-sickness and developer-persuader. Using a technique of server-side rendering and static site generation, Next provides for rapid bike acceleration and prominent search rankings, both crucial for modern web applications. It offers a whole-wheel routing which makes navigation generally easier and also has some component of Automatic code splitting for better load times. The Next. js framework not only comes with built-in support for typescript but also provides out-of-the-box solutions for styling through css in built frameworks like styled-components. Modern js provides a highly productive environment and an enhanced code quality with ease in maintainability. An app that begins as small scale projects can be a simple one for learning purpose and can be expanded into enterprise levels applications throughout the process. It makes it possible for developers to develop websites that are fast, huge, and feature-rich with relative convenience.

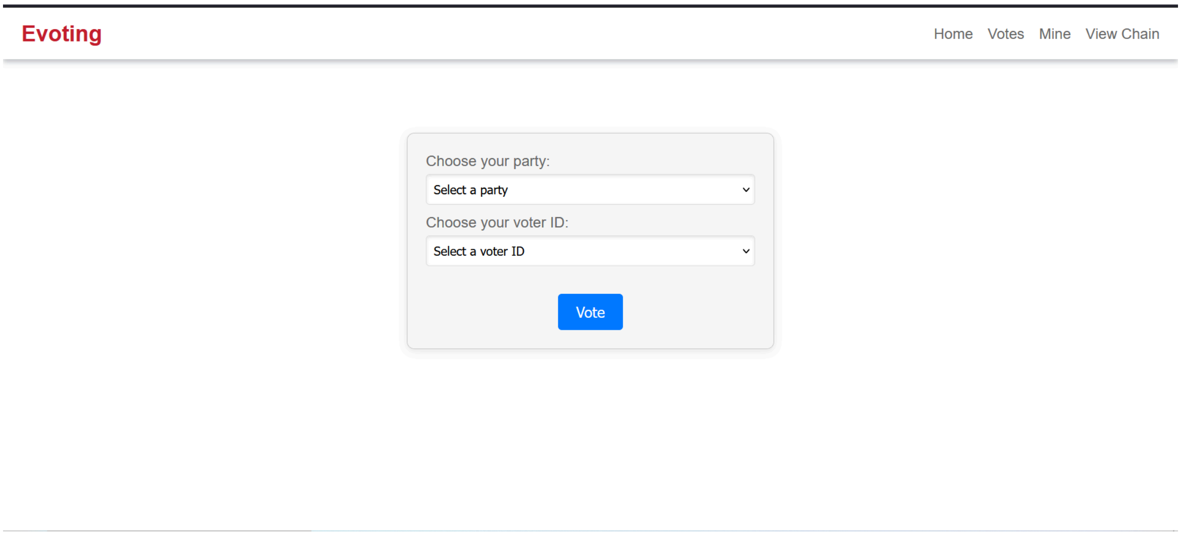
CHAPTER 5: RESULT AND EVALUATION

5.1 Results

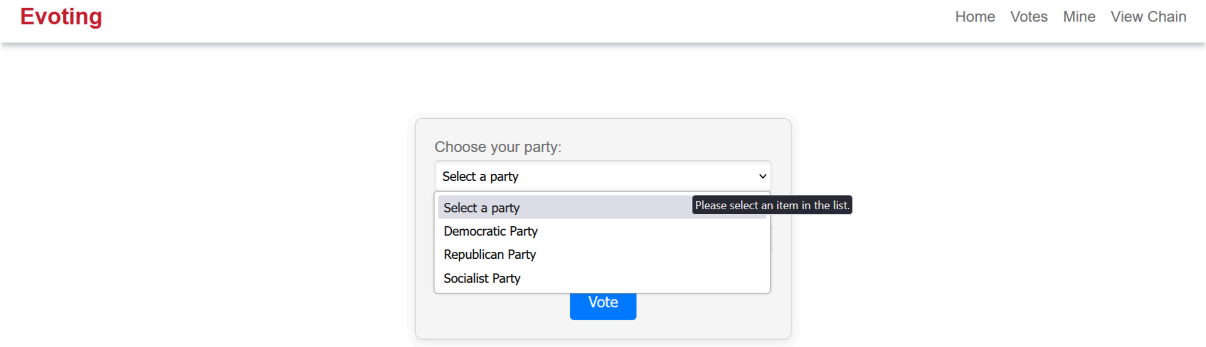
By taking everything into account, we were able to implement a voting system that shows "Voted" after every vote, promptly alerting voters to their participation. Furthermore, our system features a safety feature that shows "Already Voted" following several vote attempts. This success demonstrates our commitment to upholding the voting process's accuracy and fairness, offering a transparent and safe environment for voters, and protecting the system's integrity.Finally, we can display the voting results once the election concludes.

5.1.1 Output Snippets

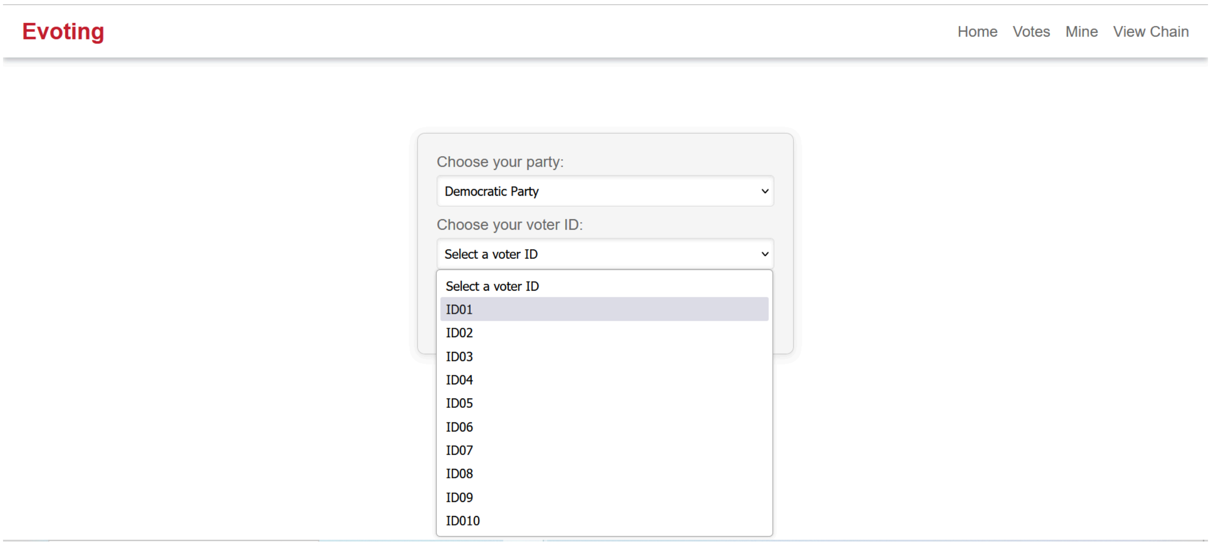
Below is the home page of the application which consists of Home button, Votes button, Mine button, View chain. This also consists of the option to select the party and the voter id.



Further, we can choose the party that we want to vote. Here, we have three options to choose from.



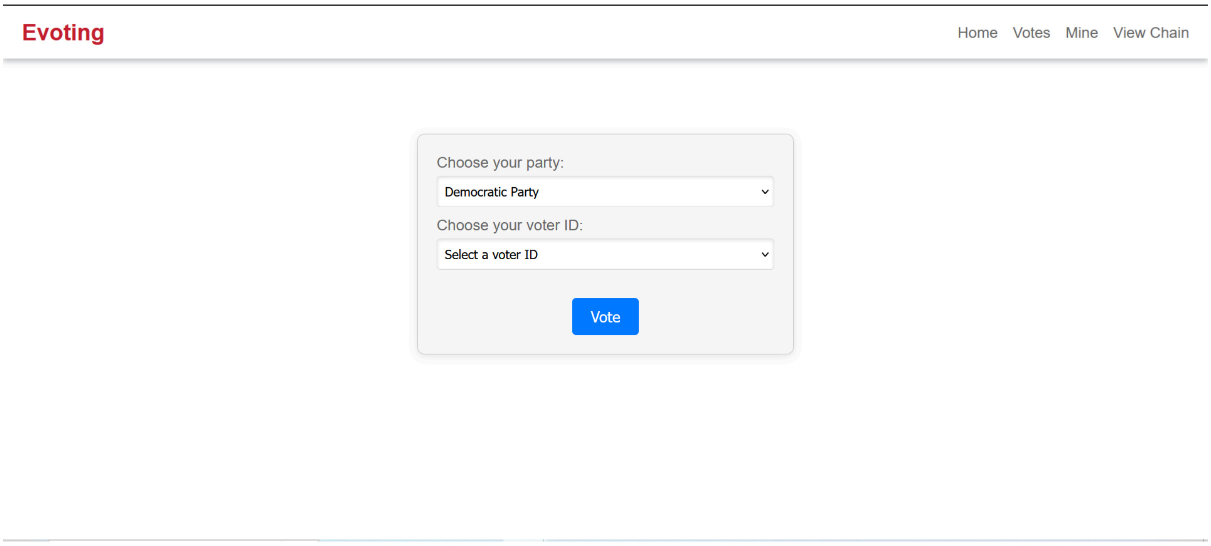
In the next step we will choose the voter id using which the voter will cast their vote.Here, we have taken 10 voter ids from which the voter can choose one.



Choose your party: Democratic Party

Choose your voter ID: Select a voter ID

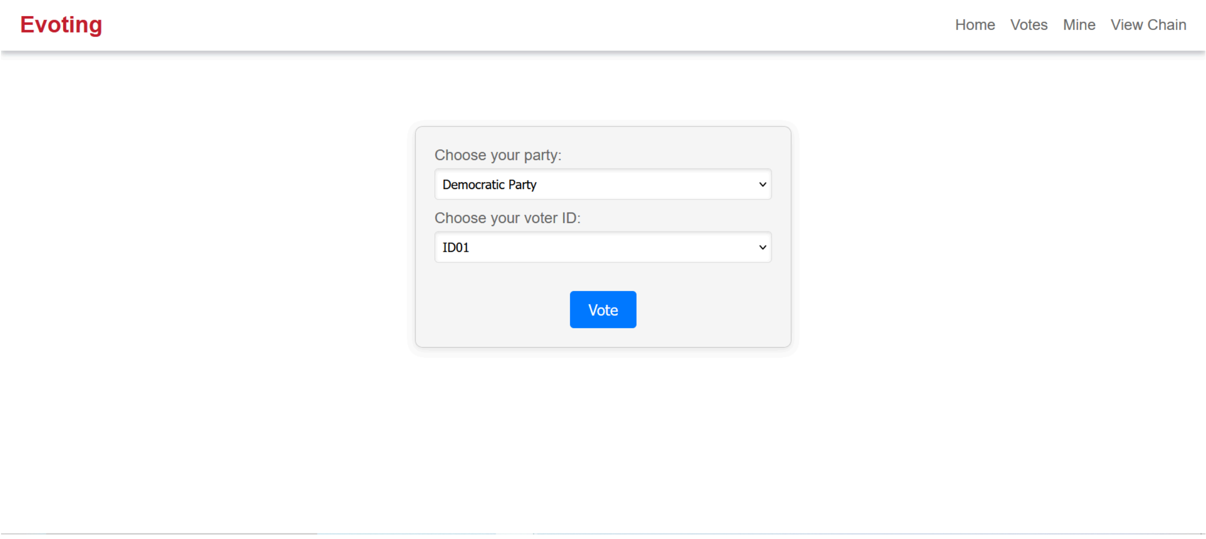
Now, we will choose the party to which our vote will be casted.



Choose your party: Democratic Party

Choose your voter ID: Select a voter ID

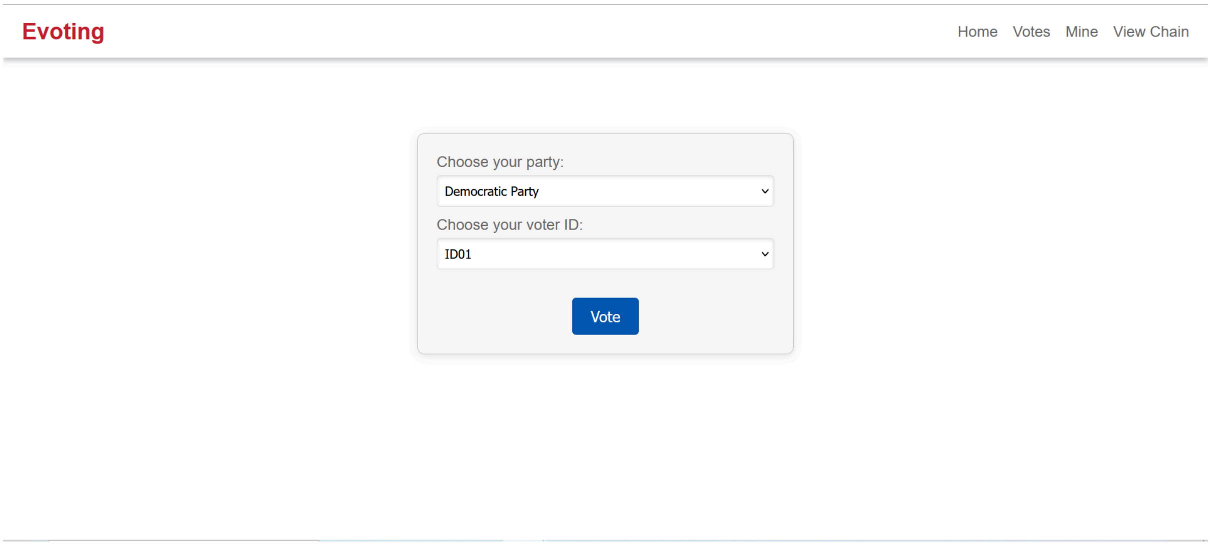
Choose the voter id using which we will cast the vote.



Choose your party: Democratic Party

Choose your voter ID: ID01

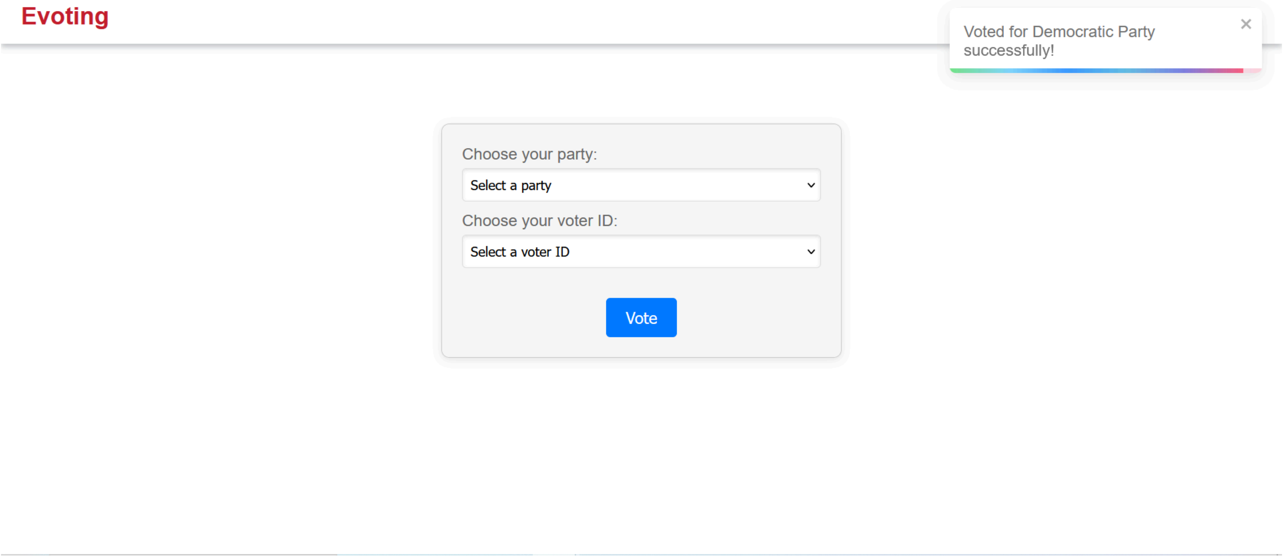
Now, click on the vote button to cast the vote to the chosen party.



Choose your party: Democratic Party

Choose your voter ID: ID01

The vote to the chosen party with the chosen voted id has been casted successfully.


Evoting

Voted for Democratic Party successfully!

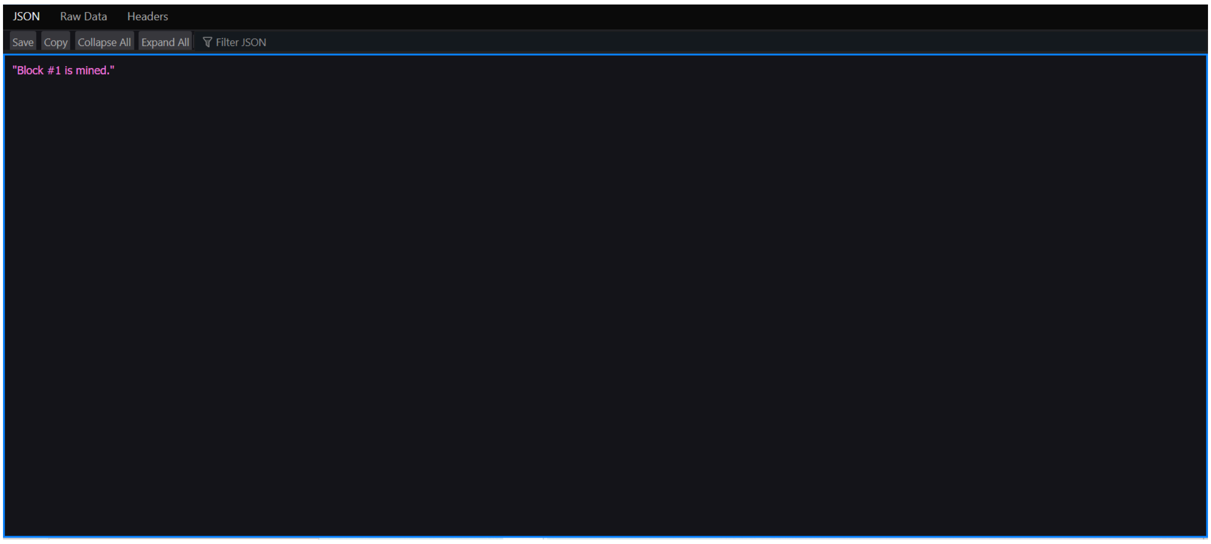
Choose your party:

Select a party

Choose your voter ID:

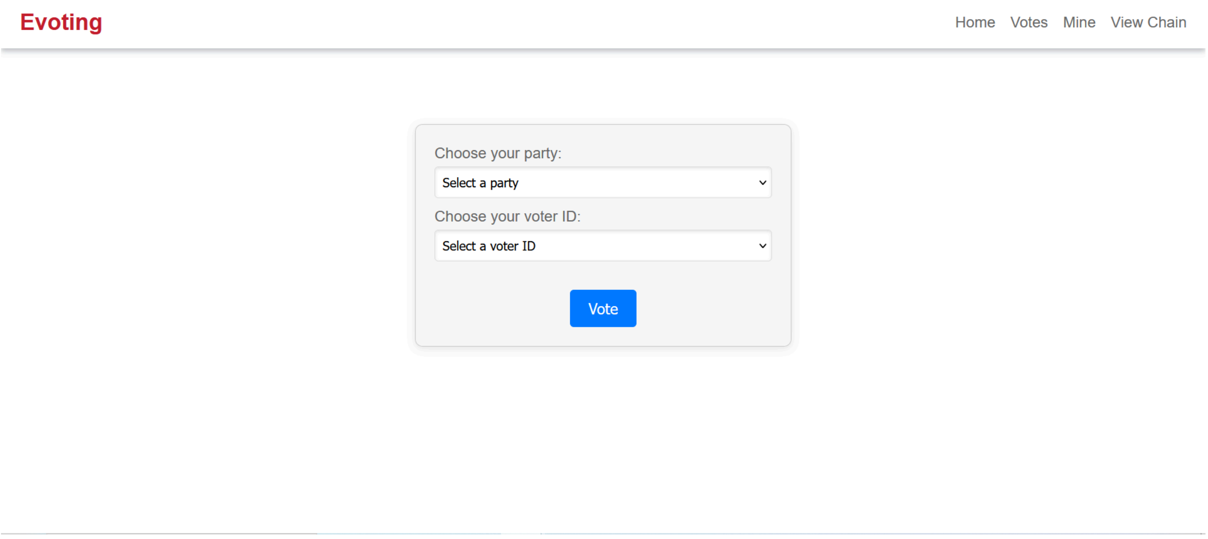
Select a voter ID

To add our vote to the blockchain network we will mine the vote. Below is the page that will load up after mining, notifying that block has been mined.



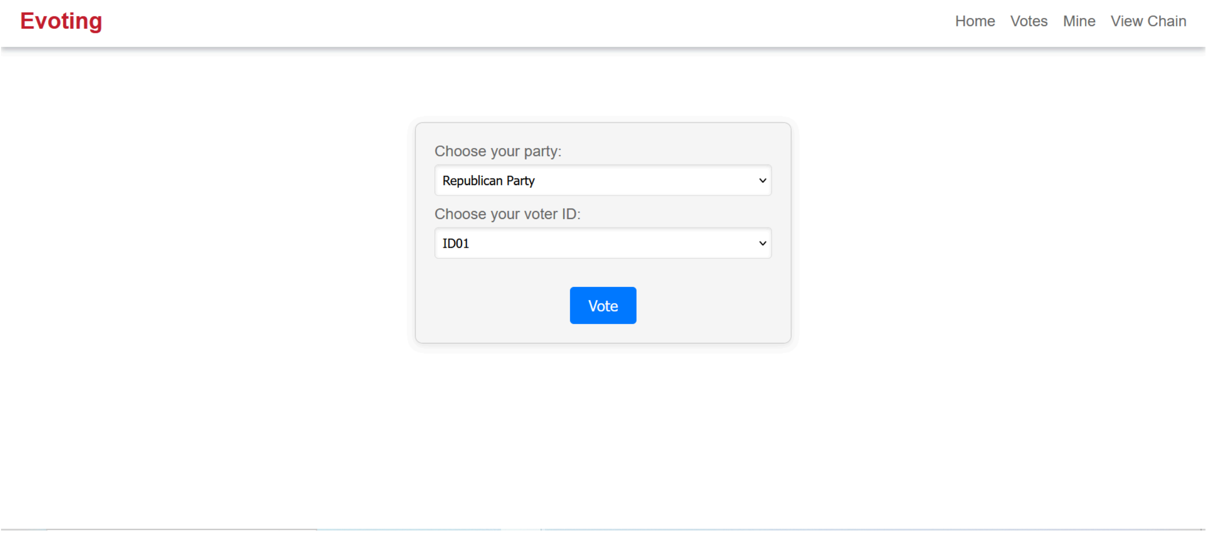
"Block #1 is mined."

After voting, the homepage will reset itself to the original form i.e we can again select the party and the voter id to vote.



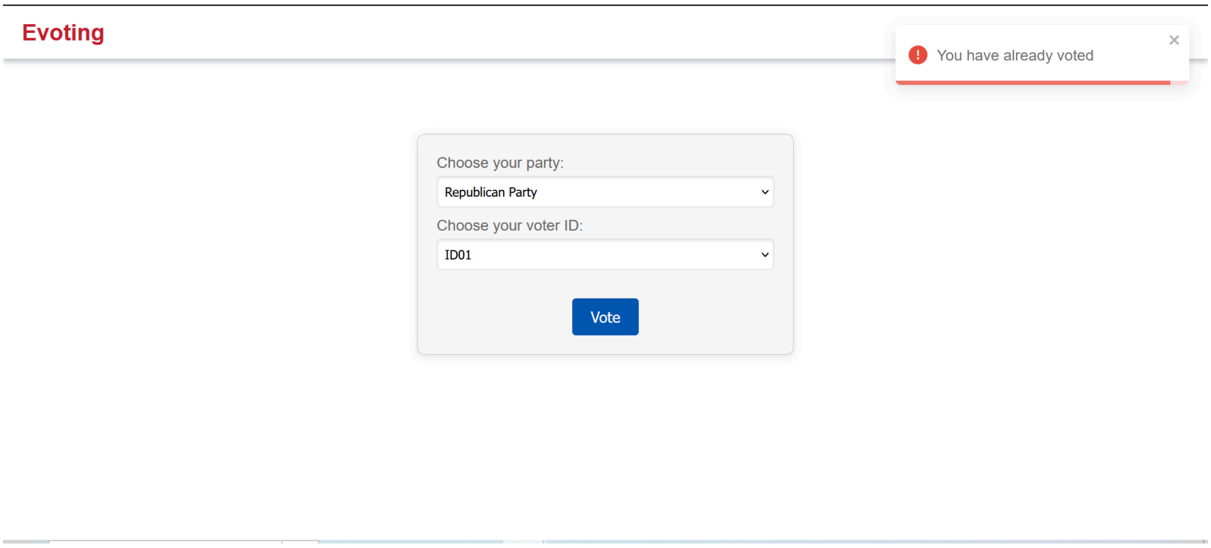
Choose your party:
Select a party
Choose your voter ID:
Select a voter ID

Here, we have taken an example of voting done by the same voter using the same id. The main aim here is to show that a voter can’t vote again.



Choose your party:
Republican Party
Choose your voter ID:
ID01

After pressing the vote button, a notification will pop-up displaying a message as “you have already voted”. Indicating that we can’t vote again.

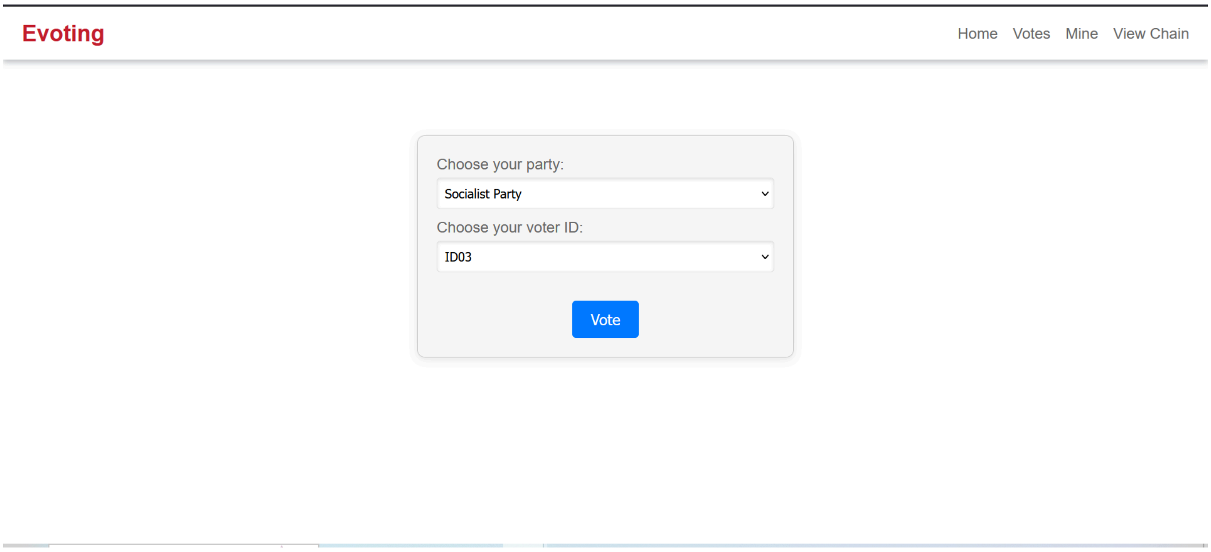


You have already voted

Choose your party: Republican Party

Choose your voter ID: ID01

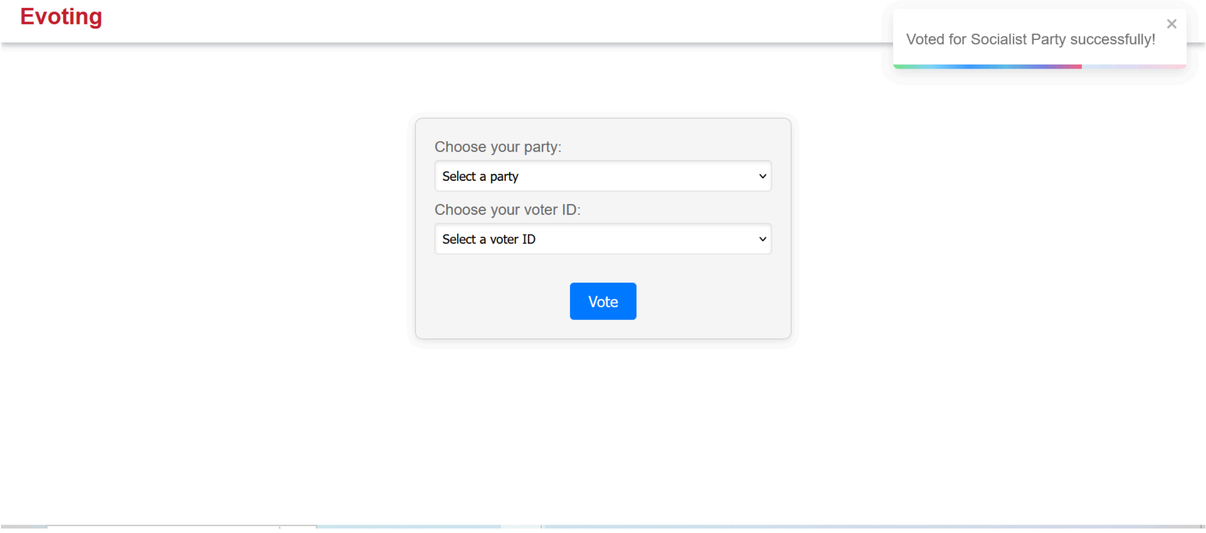
Now, we will take another example of voting to a different party using a different voter id.



Choose your party: Socialist Party

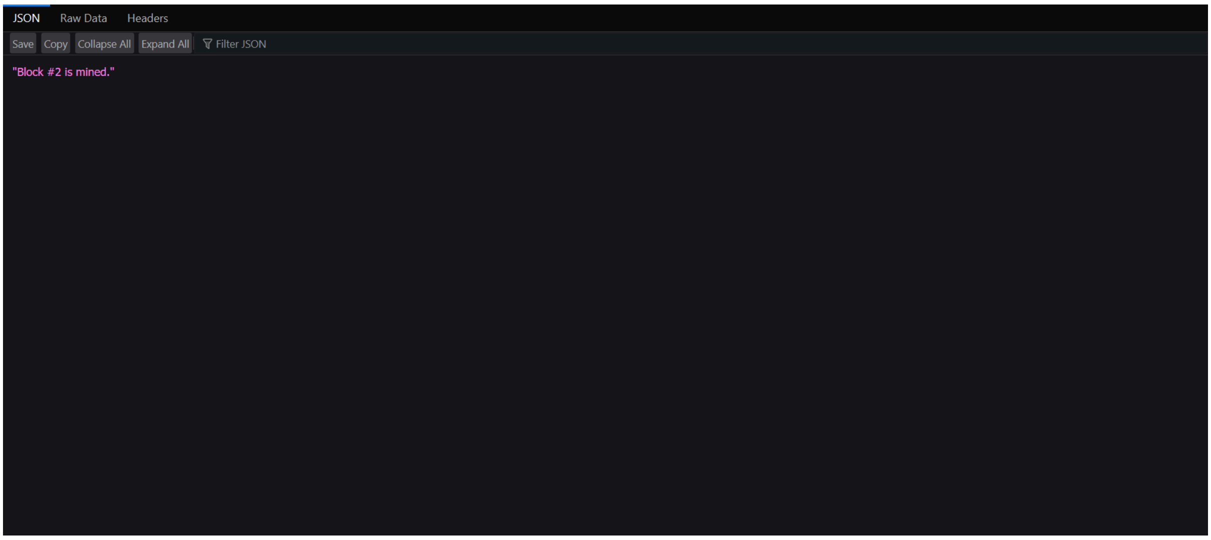
Choose your voter ID: ID03

We have successfully casted the vote using different details.



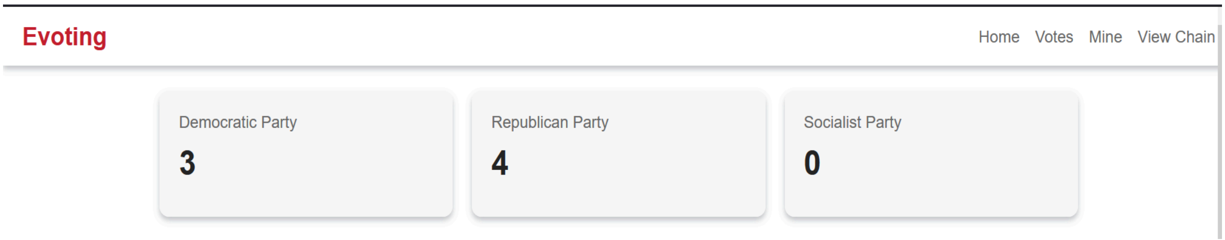
Voted for Socialist Party successfully!

Below is the notification for the mining of the second vote i.e the second vote.



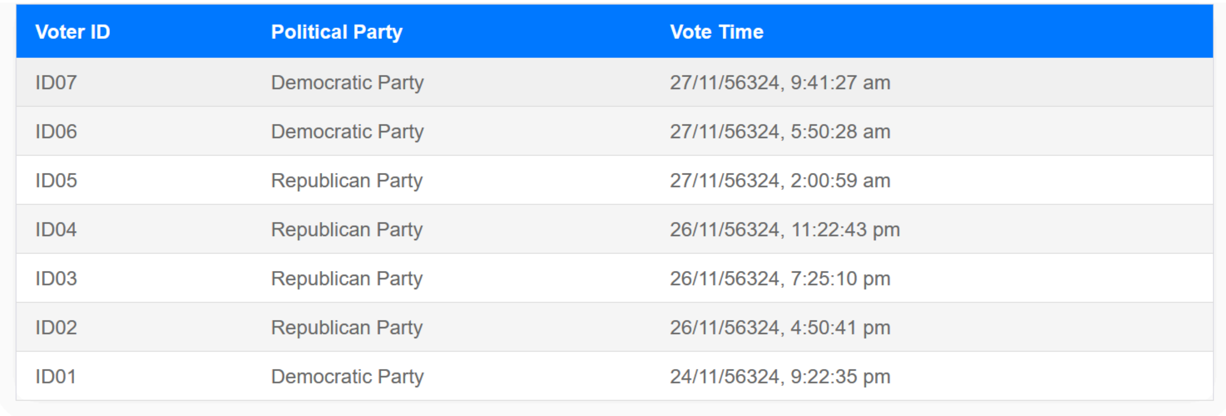
```
"Block #2 is mined."
```

After successfully casting multiple votes to different parties with multiple voter ids, below is the final result of the election showing the clear winner of the election.



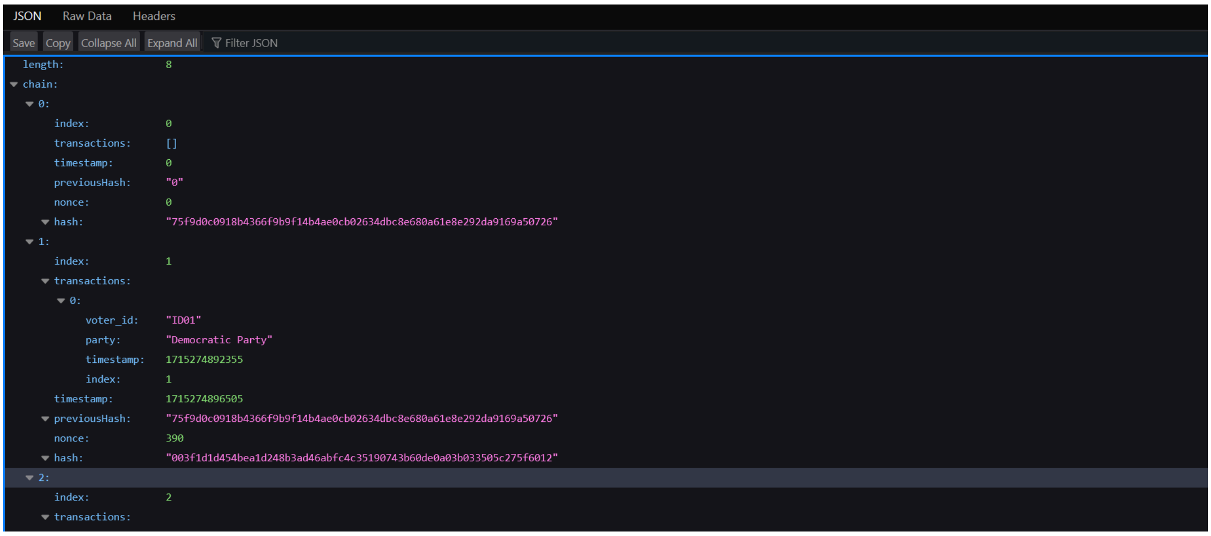
Democratic Party	Republican Party	Socialist Party
3	4	0

Here, we can see more details of the election in which voter casted the vote to the party at which time and at which date.



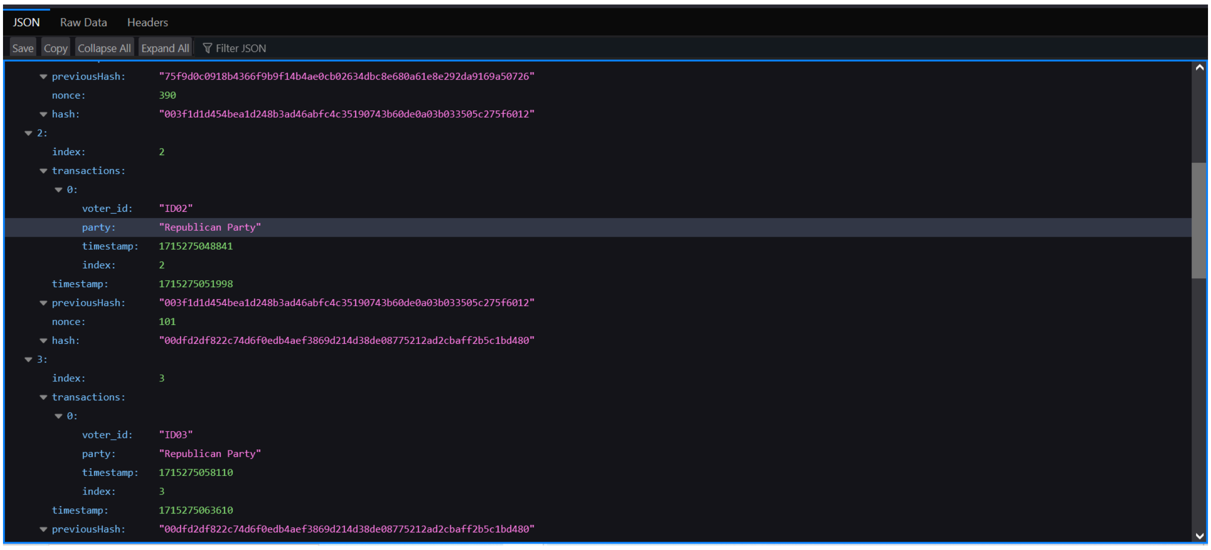
Voter ID	Political Party	Vote Time
ID07	Democratic Party	27/11/56324, 9:41:27 am
ID06	Democratic Party	27/11/56324, 5:50:28 am
ID05	Republican Party	27/11/56324, 2:00:59 am
ID04	Republican Party	26/11/56324, 11:22:43 pm
ID03	Republican Party	26/11/56324, 7:25:10 pm
ID02	Republican Party	26/11/56324, 4:50:41 pm
ID01	Democratic Party	24/11/56324, 9:22:35 pm

Following are the transactions or the creation of the nodes in the blockchain network in which we can see the details of the votes casted. This also consists of the hash values through which we can uniquely identify each node in the blockchain network.These are some of the initial transactions.



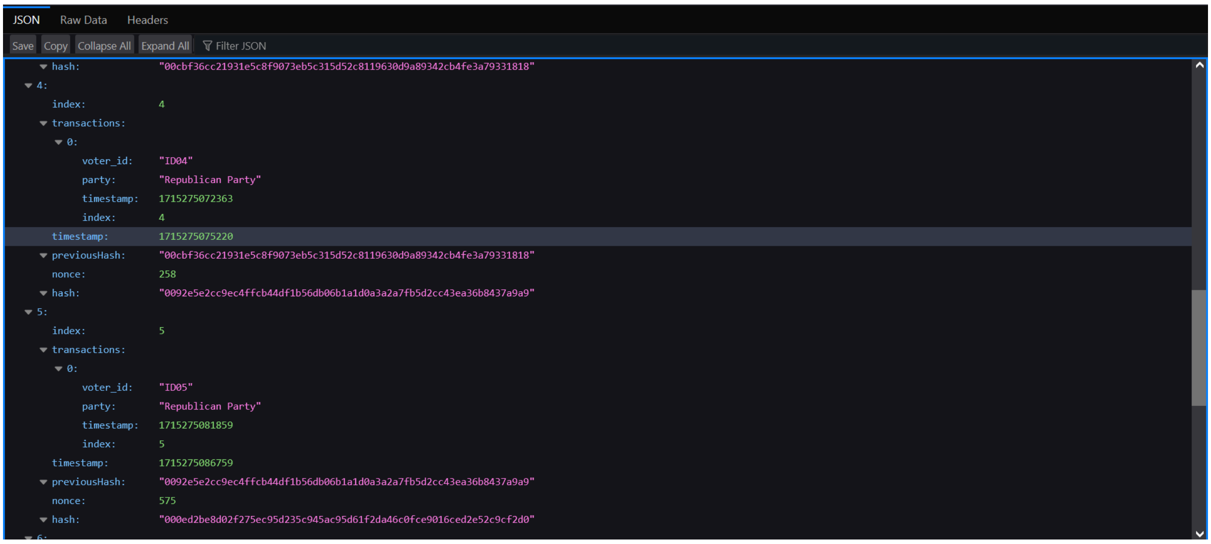
```
length:               8
chain:
  0:
      index:          0
      transactions:   []
      timestamp:      0
      previousHash:   "0"
      nonce:          0
      hash:           "75f9d0c0918b4366f9b9f14b4ae0cb02634dbc8e680a61e8e292da9169a50726"
  1:
      index:          1
      transactions:
        0:
          voter_id:   "ID01"
          party:      "Democratic Party"
          timestamp:  1715274892355
          index:      1
      timestamp:      1715274896505
      previousHash:   "75f9d0c0918b4366f9b9f14b4ae0cb02634dbc8e680a61e8e292da9169a50726"
      nonce:          390
      hash:           "003f1d1d454bea1d248b3ad46abfc4c35190743b60de0a03b033505c275f6012"
  2:
      index:          2
      transactions:
```

These are the middle transactions.



```
      previousHash:   "75f9d0c0918b4366f9b9f14b4ae0cb02634dbc8e680a61e8e292da9169a50726"
      nonce:          390
      hash:           "003f1d1d454bea1d248b3ad46abfc4c35190743b60de0a03b033505c275f6012"
  2:
      index:          2
      transactions:
        0:
          voter_id:   "ID02"
          party:      "Republican Party"
          timestamp:  1715275048841
          index:      2
      timestamp:      1715275051998
      previousHash:   "003f1d1d454bea1d248b3ad46abfc4c35190743b60de0a03b033505c275f6012"
      nonce:          101
      hash:           "00dfd2df822c74d6f0edb4aef3869d214d38de08775212ad2cbaff2b5c1bd480"
  3:
      index:          3
      transactions:
        0:
          voter_id:   "ID03"
          party:      "Republican Party"
          timestamp:  1715275058110
          index:      3
      timestamp:      1715275063610
      previousHash:   "00dfd2df822c74d6f0edb4aef3869d214d38de08775212ad2cbaff2b5c1bd480"
```

These are some more transaction.



```
    hash:              "00cbf36cc21931e5c8f9073eb5c315d52c8119630d9a89342cb4fe3a79331818"
  4:
    index:             4
    transactions:
      0:
        voter_id:      "ID04"
        party:         "Republican Party"
        timestamp:     1715275072363
        index:         4
    timestamp:         1715275075220
    previousHash:      "00cbf36cc21931e5c8f9073eb5c315d52c8119630d9a89342cb4fe3a79331818"
    nonce:             258
    hash:              "0092e5e2cc9ec4ffcb44df1b56db06b1a1d0a3a2a7fb5d2cc43ea36b8437a9a9"
  5:
    index:             5
    transactions:
      0:
        voter_id:      "ID05"
        party:         "Republican Party"
        timestamp:     1715275081859
        index:         5
    timestamp:         1715275086759
    previousHash:      "0092e5e2cc9ec4ffcb44df1b56db06b1a1d0a3a2a7fb5d2cc43ea36b8437a9a9"
    nonce:             575
    hash:              "000ed2be8d02f275ec95d235c945ac95d61f2da46c0fce9016ced2e52c9cf2d0"
  6:
```

CHAPTER 6: CONCLUSION & FUTURE SCOPE

6.1 Conclusions

It might be one of the top ways that problems with conventional electoral systems can be reduced through the incorporation of blockchain to come up with a sound e-vote. The following are key findings regarding the implementation of a secure e-voting system leveraging blockchain:

Transparency and Integrity: Open-source based blockchain validates the credibility of the election results. This will form a chain and in turn reduce the chances of traces that can be traced back.

Immutable Record: Votes can be inserted into the block chain, and once they are in, it will not be easy for one to change them. All such votes have remained unexamined thereby indicating that all the casted votes are true, correct, authentic in past.

Decentralization: Just getting rid of their weaknesses does not strengthen them. It simply weakens them in comparison with a central system. Adds intensity and strength to the mandate and performance of the elective. Security through Cryptography: In order to achieve the needs of voter's privacy, confidentiality, anonymity, as well as secrets – cryptographic measures such as encryption, as well as digital signature are used.

Anonymity and Voter Privacy: Secret balloting method via cryptography-based cryptograms such as e-voting.

Accessibility: E-voting may provide a more practical means of voting for disabled and rural area voters. User experience could just involve a single click at an online Vote.

Reduced Intermediaries: This does away with using any other proxies prior to the voting process. Smart contracts make this possible. Some defects associatedwith manual work come from a certain part of the voting procedure, which they can handle.

Auditability: Blockchain as such is transparent and auditable therefore empowering stakeholders to independently verify the result of elections using it. All information registered in the chain is visible for everyone who has access to it.

Resistance to Cyber Attacks: Highly trustable consensus protocols and secure source code of Blockchain based e-voting system helps it resist the most common cyber threats. This gives the architecture hierarchical setup and hence, for an attacker, it would be difficult to penetrate all entities simultaneously. Challenges and Considerations: These are not without problems in a securely cast vote inside a blockchain. This involves securing the fundamental level of the blockchain, solving the contracts problems, and managing compliance and acceptance obstacles.

Testing and Verification: Adequate testing, as well as audit procedures for blockchain protocol and smart-contract. Another way through which this is achieved is by carrying out second level independent verification and validation, thereby reinforcing the integrity of the electronic voting. Finally, implementing blockchains should be done after considering technical issues, governance problems, security issues as well as the legal aspects involved. Discussing such factors towards e-voting will be certain and foreseeable

6.2 Future Scope

1. **Scalability Solutions:**
   Problems with scaling systems should be looked at so that vote production and transactions of blockchain voting systems can be sustained as the global increase of voters. The new technology either requires the complex scaling mechanisms dedicated for the e-voting environment or the technique has to present a solution to this issue by creating novel scaling methods. One of the most applicable technologies that may boost the totally is blockchain sharding. This may be performed by partitioning the blockchain into smaller blocks. Thus, congestion of the blockchain network and lowering its throughput can be reduced. Next protocols can be built with a collection of state networks to relay chains or side chains which can facilitate scaling operations as well as processing of transactions to happen away from the main chain without mortgaging the chains overall security.

2. **User-centric design and accessibility:**

   Electronic voting systems interface design especially in terms of amongst the users acceptance and friendly operation also is not less important. It is however the future solutions of campaign strategies should be subsequently reflected on a user-friendly web application that is responsive, custom-built, and flexible enough to accommodate the changing needs and motives of the electorates. This objective can be achieved by throughput of comprehensive usability testing from the agents that are going to be involved in the implementation of the virtual company slowly and gradually which is an option to make the platform more and more efficient. The method for deploying the voting system, such as mobile apps, papers ballots with Optical Character Recognition (OCR), and remote voting, need to be in the platform. These are the two significant discouragements associated with the transport and living conditions in different regions that will be now avoided thanks to this realization.

3. **Transparency, audibility, and trust:**

   The fair and free elections that are meticulously scrutinized by the authorities that are responsible and accountable are in this case. While the rank of responsibility in the hierarchy of importance is increasing, the need of its importance, as well, is growing. To some extent, the latter stands out because it implies recording of the book items which cannot be changed. At the same time, conversely, the entries into the ledger are traceable and transparent, thus, supporting the general trust from the public. In the same manner, the redesigned voting as well as election systems ought to have the prominent elements of openness, transparency, and accountability. This, will, in turn, build the trust and confidence of the voters. Public trust in fair and neutral election body can be acquired by the provisions of public scrutiny made of the basic open audit when voting starts, the impartial review of the final results, and intensive scrutiny that can be made to look in to. Implying that if the educational system is set up in such way that the voters and also the other stakeholders who cannot understand the auditability of the electoral system due to lack of the knowledge of the blockchains usage, the popularity of the voting systems will be on rise.

References:

[1]S. Kavitha, Praveen. R, Ragavendrar. M.A, Vishwa., 2023. Online E-Voting System Using Blockchain Technology. In *International Journal for Research and Applied Science and Engineering Technology (IJRASET)* (pp. 1-5).

[2] Samruddhi Pawar, Aachal Sahare, Snehal Shelar, Pranjali Bagal and Prof. S. S Dixit,2023. Secure E-Voting system using Blockchain Technology *(IJRASET)* (pp. 1-5).

[3] Namrata Jaiswar1 , Soham Deodhar2 , Harish Gupta3 and Prof. Dnyaneshwar Kapse4, 2023. (GCAT) E-Voting system using Blockchain(pp. 1-4)

[4] Yutesh Mohadikar, Sumedh Wasnik, Sarthak Malpani, Abhilasha Lokhande, Ashwini Shinde and Priya Sudewad, 2022. E-voting system using Block-Chain.(IJRASET) pp.1-9.

[5] Bindewari, S. and Surana, J., 2019. Design and Implementation a Smart E-Voting Model: Decentralization Using Blockchain.

[6] Pandey, A., Bhasi, M. and Chandrasekaran, K., 2019, October. VoteChain: A Blockchain based e-voting system. In *2019 Global Conference for Advancement in Technology (GCAT)* (pp. 1-4). IEEE.

[7] Shahzad, B. and Crowcroft, J., 2019. Trustworthy electronic voting using adjusted blockchain technology. *Ieee Access*, *7*, pp.24477-24488.

[8] Gao, S., Zheng, D., Guo, R., Jing, C. and Hu, C., 2019. An anti-quantum e-voting protocol in blockchain with audit function. *IEEE Access*, *7*, pp.115304-115316.

[9]Yi, H., 2019. Securing e-voting based on blockchain in P2P network. *EURASIP Journal on Wireless Communications and Networking*, *2019*(1), pp.1-9.

[10] Adeshina, S.A. and Ojo, A., 2019, December. Maintaining voting integrity using blockchain. In *2019 15th International Conference on Electronics, Computer and Computation (ICECCO)* (pp. 1-5). IEEE.

[11] Kshetri, N. and Voas, J., 2018. Blockchain-enabled e-voting. Ieee Software, 35(4), pp.95-99.

[12] Ayed, A.B., 2017. A conceptual secure blockchain-based electronic voting system. International Journal of Network Security & Its Applications, 9(3), pp.01-09.

[13] Onecoin. Retrieved 26 8, 2018, from https://peakd.com/blockchain/@onecoinpk/top-25-blockchain-quotes-in-2018

[14] Brave New Coin. Retrieved 22 8, 2018, from https://bravenewcoin.com/.

[15] Nakamoto, S. Retrieved 22 8, 2018, from http/bitcoin.or /bitcoin.pdf., 2008.

[16] Blockchains & Distributed Ledger Technologies. Retrieved 22 8, 2018, from https://blockchainhub.net/

[17] Smart Contracts. Retrieved 26 8, 2018, from http://blockchainhub.net/

[18] PwC. Retrieved 26 8, 2018, from http/www.pwc.in/

[19] Hjálmarsson, F.Þ., Hreiðarsson, G.K., Hamdaqa, M. and Hjálmtýsson, G., 2018, July. Blockchain-based e-voting system. In 2018 IEEE 11th international conference on cloud computing (CLOUD) (pp. 983-986). IEEE.

[20] Zhang, S., Wang, L. and Xiong, H., 2020. Chaintegrity: blockchain-enabled large-scale e-voting system with robustness and universal verifiability. International Journal of Information Security, 19, pp.323-341.

[21] Sadia, K., Masuduzzaman, M., Paul, R.K. and Islam, A., 2019. Blockchain based secured e-voting by using the assistance of smart contract. arXiv preprint arXiv:1910.13635.

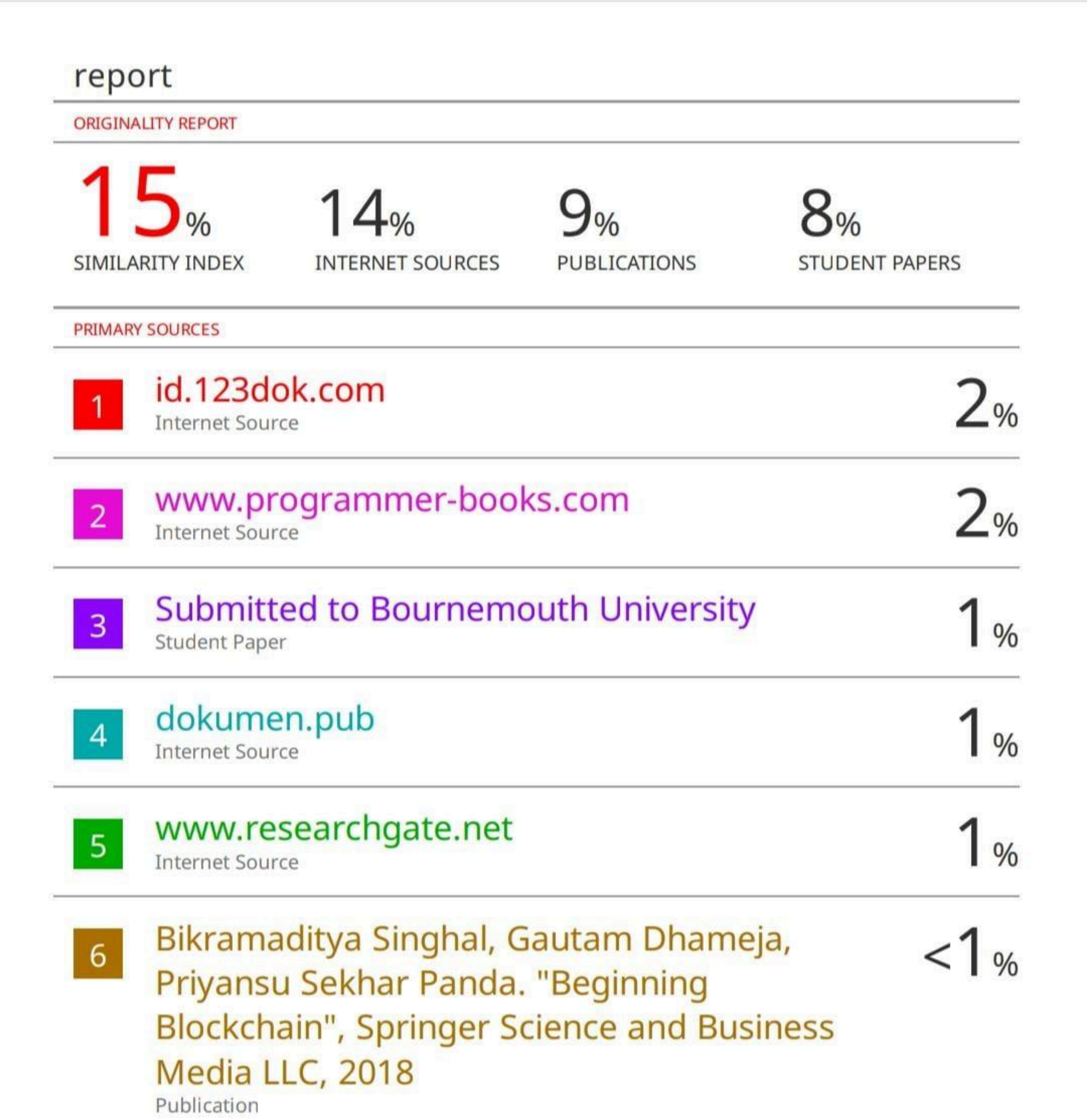
[22] Patil, H.V., Rathi, K.G. and Tribhuwan, M.V., 2018. A study on decentralized e-voting system using blockchain technology. Int. Res. J. Eng. Technol, 5(11), pp.48-53.

[23] Braghin, C., Cimato, S., Cominesi, S.R., Damiani, E. and Mauri, L., 2019. Towards blockchain-based e-voting systems. In Business Information Systems Workshops: BIS 2019 International Workshops, Seville, Spain, June 26–28, 2019, Revised Papers 22 (pp. 274-286). Springer International Publishing.

[24] Hsiao, J.H., Tso, R., Chen, C.M. and Wu, M.E., 2018. Decentralized E-voting systems based on the blockchain technology. In Advances in Computer Science and Ubiquitous Computing: CSA-CUTE 17 (pp. 305-309). Springer Singapore.

[25] Kovic, M., 2017. Blockchain for the people: Blockchain technology as the basis for a secure and reliable e-voting system.

APPENDIX



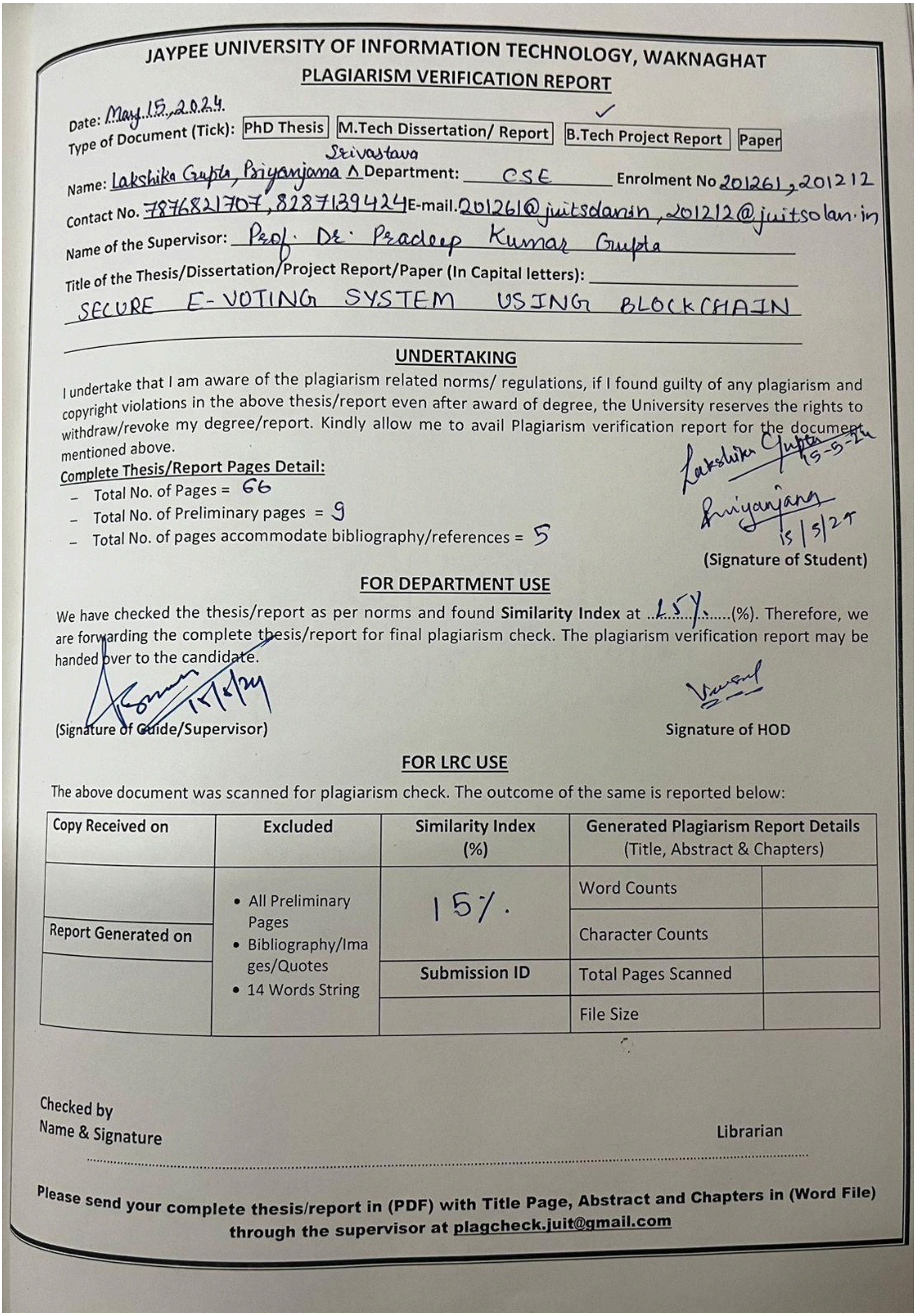
report

ORIGINALITY REPORT

15%	14%	9%	8%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	id.123dok.com Internet Source	2%
2	www.programmer-books.com Internet Source	2%
3	Submitted to Bournemouth University Student Paper	1%
4	dokumen.pub Internet Source	1%
5	www.researchgate.net Internet Source	1%
6	Bikramaditya Singhal, Gautam Dhameja, Priyansu Sekhar Panda. "Beginning Blockchain", Springer Science and Business Media LLC, 2018 Publication	<1%



JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

PLAGIARISM VERIFICATION REPORT

Date: May 15, 2024

Type of Document (Tick): PhD Thesis | M.Tech Dissertation/ Report | [✓ B.Tech Project Report] | Paper

Name: Lakshika Gupta, Priyanjana Srivastava Department: CSE Enrolment No 201261, 201212

Contact No. 7876821707, 8287129424 E-mail. 201261@juitsolan.in, 201212@juitsolan.in

Name of the Supervisor: Prof. Dr. Pradeep Kumar Gupta

Title of the Thesis/Dissertation/Project Report/Paper (In Capital letters): SECURE E-VOTING SYSTEM USING BLOCKCHAIN

UNDERTAKING

I undertake that I am aware of the plagiarism related norms/ regulations, if I found guilty of any plagiarism and copyright violations in the above thesis/report even after award of degree, the University reserves the rights to withdraw/revoke my degree/report. Kindly allow me to avail Plagiarism verification report for the document mentioned above.

Complete Thesis/Report Pages Detail:

- Total No. of Pages = 66
- Total No. of Preliminary pages = 9
- Total No. of pages accommodate bibliography/references = 5

Lakshika Gupta 15-5-24

Priyanjana 15/5/24

(Signature of Student)

FOR DEPARTMENT USE

We have checked the thesis/report as per norms and found **Similarity Index** at 15%(%). Therefore, we are forwarding the complete thesis/report for final plagiarism check. The plagiarism verification report may be handed over to the candidate.

15/5/24

(Signature of Guide/Supervisor) Signature of HOD

FOR LRC USE

The above document was scanned for plagiarism check. The outcome of the same is reported below:

Copy Received on	Excluded	Similarity Index (%)	Generated Plagiarism Report Details (Title, Abstract & Chapters)	
	• All Preliminary Pages • Bibliography/Images/Quotes • 14 Words String	15%.	Word Counts	
Report Generated on			Character Counts	
		Submission ID	Total Pages Scanned	
			File Size	

Checked by
Name & Signature Librarian

Please send your complete thesis/report in (PDF) with Title Page, Abstract and Chapters in (Word File) through the supervisor at plagcheck.juit@gmail.com